IFAL: Issue First Activate Later Certificates for V2X

Eric R. Verheul[†], Christopher Hicks[*], Flavio D. Garcia[*]
[†]Radboud University, Nijmegen, The Netherlands
eric.verheul@cs.ru.nl
[*]School of Computer Science, University of Birmingham, United Kingdom
{c.hicks, f.garcia}@cs.bham.ac.uk

***Abstract*—This paper presents IFAL, a provably secure and privacy conscious scheme for Vehicle-to-Vehicle and Vehicle-to-Infrastructure (V2X) communication. Issue First Activate Later (IFAL) is a practical and secure improvement to the leading European candidate for V2X (ETSI) and one that also merits over the leading US standard. IFAL incorporates a novel cryptographic mechanism that both avoids the need for certificate revocation and which supports vehicles with limited and intermittent connectivity. We introduce a new construction that is equivalent to symmetric key diversification in the public key setting with short, time-delayed activation. We also present a new formalisation of V2X security and privacy which we apply to IFAL to show that it is a provably secure and privacy conscious V2X scheme. IFAL is ETSI compliant and ready for integration into the standard.**

I. Introduction

Vehicle-to-Vehicle and Vehicle-to-Infrastructure (V2X) communication introduces a number of conflicting requirements which make the design of Intelligent Transportation Systems (ITS) particularly challenging [1]. Close-range vehicle linkability is a key feature of V2X that enables enhanced situational awareness and which makes V2X a viable safety feature. ITS must harmonise the requirement for close-range linkability, vehicle authentication and accountability with the need to adequately protect the vehicle owner from the type of long-term tracking that threatens to uniquely identify their individual habits.

Long-term tracking data from ride-hailing services such as Uber has been misused to facilitate corporate espionage [2], track the whereabouts of important persons and to identify customers engaging in one-night stands [3]. It is therefore highly important that ITS are designed to prevent similar attacks being performed against connected cars executing standard protocols. The European Data Protection Working Party have identified the legal requirement for protection in relation to ITS vehicle data and have specifically called for new measures which limit the risks of long-term vehicle tracking [4].

The two main Public Key Infrastructure (PKI) proposals for ITS are the European Telecommunications Standards Institute (ETSI) standardised approach [5] and the U.S. Department of Transportation (USDOT) approach based on the Secure Credential Management System (SCMS) [6]. The Institute of Electrical and Electronics Engineers (IEEE) Wireless Access in Vehicular Environments (WAVE) standard [7] provides the common V2X message structure that is used by both of the main ITS proposals. The adoption of these standards is strongly encouraged by a European Parliament ITS Directive [8] which mandates interoperable communication between vehicles. Volkswagen, Toyota, General Motors and Daimler have already announced that they are using ETSI and WAVE standards for V2X communication [9].

Both the ETSI and USDOT PKI systems use a number of Certificate Authorities (CA) and Certificate Revocation Lists (CRL) to manage the credentials of vehicles. Privacy is managed by issuing each vehicle a long-term authorisation certificate and an additional number of short-term pseudonymous certificates which are used to sign V2X messages. Drivers are held accountable by an authority who can compel the certificate authorities to collude and link a pseudonym certificate with the registered owner of a vehicle.

It is particularly important that ITS PKI supports the revocation of credentials from misbehaving entities which send incorrect information. Both ITS standards use the CRL method for revoking credentials, effectively a blacklist of revoked credentials that is checked during each signature validation. The CRL method suffers from several drawbacks, including that the size is likely to grow very large given the anticipated scale of vehicular networks. Large CRL are particularly problematic when considering the latency between receiving a signed message and verifying that the corresponding certificate has not been revoked.

In recognition of the shortcomings of CRL in an ITS environment, the USDOT ITS standard uses linkage-based revocation [10] which reduces the size of the CRL to just one key per vehicle. However, with around 300 million registered cars in each of Europe and America, limited vehicle resources and tight signature processing constraints, this is still far from ideal. The ETSI standard is yet to finalise a revocation mechanism.

A. Our Contribution

The main contributions of this paper are:

- Our new IFAL V2X scheme, which is fully compliant with the ETSI standard and has additional features such as the ability to pre-issue pseudonym certificates that are only usable upon receiving small activation codes (via

e.g. SMS). IFAL offers a much greater flexibility with regards to vehicle connectivity and furthermore avoids the need for certificate revocation which does not scale and is hard to implement in real-time systems.
- The first formalisation of the security and privacy requirements set out in the ETSI ITS standard, in a provable security setting.
- A new key diversification mechanism with time-delayed activation in the public-key setting which may have applications beyond V2X.

B. Related Work

The ETSI ITS architecture [5] was developed from a number of earlier projects [11], including SeVeCom which developed many of the initial solutions for secure V2X communication [12]. The Car2Car Communication Consortium (C2C-CC) was influential in motivating the development of the ETSI ITS standards [13]. The ISO/TC204 [14] and IEEE 1609 WAVE [7] standards are important complimentary contributions that have been developed in parallel. The EVITA project developed a secure onboard vehicular system architecture that incorporates a hardware security module (HSM) for performing cryptographic operations [15]. The PRESERVE project developed a 'close-to-market' V2X implementation that integrates the EVITA onboard vehicle architecture with a broad range of other projects and standards including ETSI ITS [16].

In the US, SCMS [6] is the leading candidate architecture for V2X. SCMS is currently in the proof-of-concept development stage and is expected to be finalised in late 2020 [17]. SCMS shares a number of similarities with the ETSI ITS standard, however it uses an implicit certificate [18] based PKI which is incompatible with IFAL certificates. Implicit certificates save storage and transmission space by omitting the public key which they authenticate. In contrast to explicit certificates, implicit certificates have received relatively little cryptographic scrutiny [18] and are the subject of a number of patents [19], [20], [21] which risk misuse by means of becoming standard-essential [22].

Pseudonyms for vehicle privacy in V2X were first proposed by the SeVeCom project [12] and have been adopted by both of the leading V2X architectures [5], [7], [6]. ETSI have yet to standardise a certificate change strategy but recently published a survey of candidate methods in [23]. SCMS implements the C2C-CC pseudonym certificate pooling approach [24] in which there are 20-40 simultaneously valid vehicle credentials. It has been shown that even so-called 'perfectly unlinkable' pseudonym change strategies that use a different pseudonym for every message are vulnerable to attacks that use Multi-Hypothesis-Tracking to link position and trajectory from different messages [25]. Achieving k-anonymity has been attempted using silent periods [26], [27] and mix-zones [28], [29] but these techniques trade system safety and availability for privacy by introducing the possibility of V2X messages that are not transmitted or unable to be recovered, respectively.

Both leading V2X standards use role separation to provide unlinkability between different vehicle pseudonym certificates. In the event of vehicle misbehaviour, certificate authorities are expected to collaborate in order to resolve the canonical vehicle identity which can then have its certificates withdrawn. The REWIRE revocation protocol [30] uses trusted computing to provide enhanced vehicle privacy that avoids the need for pseudonym resolution. Under the assumption of trusted computing onboard each vehicle, REWIRE has the advantage of providing privacy against malicious and collaborating certificate authorities. The OTOKEN protocol is an extension of REWIRE that incorporates the results of formally analysing the original protocol [31]. The PUCA architecture builds upon the C2C-CC pseudonym scheme and the REWIRE revocation protocol by using anonymous credentials between vehicles and pseudonym certificate authorities to provide 'full anonymity for honest users' [32]. In further developments, Direct Anonymous Attestation (based on group signatures) has been applied to remove the pseudonym certificate authority altogether by allowing vehicles to generate their own pseudonyms [33]. Both REWIRE and PUCA assume that the vehicle trusted computing platform cannot be compromised, and that the vehicle computer will reliably deliver revocation messages to the trusted platform, as they decentralise trust from the certificate authorities to the vehicles.

IFAL provides an improvement to the ETSI ITS security architecture that avoids the need for certificate revocation by introducing pre-issued pseudonym certificates that are only usable upon receiving small activation codes (e.g. via SMS). IFAL defines a certificate change strategy that is less susceptible to impersonation attacks [34] than the C2C-CC pseudonym certificate pooling approach [24] adopted by the US standards [6]. Lastly, IFAL retains the centralised control over vehicle revocation which is lost by some of the more privacy-friendly and less standards-compliant architectures [32], [33].

II. PRELIMINARIES

This section introduces notation and the syntax and security definitions for key derivation functions and digital signature schemes. Most of it is standard, we refer the reader to Krawczyk [35] and Goldreich [36], respectively, for a more thorough explanation.

A. Notation

With respect to encryption we use subscripted lower case k's to refer to symmetric encryption keys and subscripted upper case P's to refer to public keys. Correspondingly, we use $\mathtt{enc}(k_i, m)$ and $\mathtt{ENC}(P_i, m)$ to refer to the symmetric and public key encryption of the arbitrary message m under keys k_i and P_i, respectively. We use $\mathtt{Hash}(m)$ to denote a secure hash function applied to a message m. When choosing an element k uniformly at random from a set K we write $k \xleftarrow{\$} K$. To distinguish between group and scalar multiplication we use '$\times$' and '$*$' respectively.

Where s is a bitstring of length n, we define $|s| = n$. Where q is either prime or an order of 2, and n is prime and greater than 2^{160}, we use C to denote an elliptic curve over a finite field $\mathbb{F}_q$, and we use G to denote a point on the curve which generates a cyclic subgroup of order n under addition. We require that the discrete logarithm problem in the subgroup spanned by G is hard.

In the formal setting we use the term t to refer to some infeasible computational duration and the term ε to mean some negligible quantity such that t/ε is greater than the running time of any feasible attacker.

B. Digital Signature Scheme

Formally, a digital signature scheme is a triple $(\mathcal{G}, \mathcal{S}, \mathcal{V})$ of efficient algorithms, where

- $\mathcal{G}$ is a *key-generation algorithm* that takes as input the security parameter η and outputs a pair of bitstrings (s, v) which are the signing and verification keys respectively;
- $\mathcal{S}$ is a *signing algorithm* which takes as input a signing key s and a message m and outputs a signature σ on the message m;
- $\mathcal{V}$ is a *verification algorithm* that takes as input a verification key v, a signature σ, and a message m, and outputs `true` if σ is a valid signature on m.

The standard security definition for digital signature schemes is *existential forgery on adaptively chosen message attacks* (EUF-CMA) [38]. The definition refers to an experiment that is played between an efficient adversary $\mathcal{A}$ and an oracle $\mathcal{O}_{\mathcal{S}}$ that will sign arbitrary messages. The public-key signature scheme experiment is defined as follows:

EUF-CMA$_{\mathcal{O}_{\mathcal{S}}}(1^\eta, \mathcal{A})$:

1) The oracle $\mathcal{O}_{\mathcal{S}}$ simulates the key-generation algorithm G which generates the key pair (k, P) and then provides the adversary $\mathcal{A}$ with the target verification key $P^\star$.
2) Challenge: Polynomially many times, the adversary $\mathcal{A}$ submits a message m to the oracle $\mathcal{O}_{\mathcal{S}}$ and learns the corresponding signature $\sigma = \mathcal{O}_{\mathcal{S}}(k, m)$.
3) Output: The adversary $\mathcal{A}$ outputs the pair of bitstrings $(m^\star, \sigma^\star)$.

The adversary $\mathcal{A}$ is deemed successful and wins the EUF-CMA experiment only if the following two conditions hold

1) The message $m^\star$ is different from all queries made by the $\mathcal{A}$ to the signing oracle $\mathcal{O}_{\mathcal{S}}$. In other words, $m^\star$ is different from any string in $\mathcal{O}_{\mathcal{S}}(k, m)$.
2) The tuple $(m^\star, \sigma^\star)$ corresponds to a valid message-signature pair relative to the verification key $P^\star$ and therefore $\mathcal{V}(P^\star, m^\star, \sigma^\star) = 1$.

Definition 1 (Secure Signature Scheme)**.** A digital signature scheme $\Sigma = (\mathcal{G}, \mathcal{S}, \mathcal{V})$ is said to be secure if for all efficient adversaries $\mathcal{A}$, the probability of $\mathcal{A}$ winning the experiment **EUF-CMA**$_{\mathcal{O}_{\mathcal{S}}}(1^\eta, \mathcal{A})$ is a negligible function of the security parameter η.

C. Key Derivation Function

A KDF is a function that is used to generate strong pseudorandom keys from some cryptographically inadequate initial source of keying material. Specifically, a KDF is an algorithm $\mathcal{K}$ that takes as input a bitstring k and a length parameter l. Optionally, a salt value r and a context variable x are also input. The algorithm outputs a bitstring of length l bits.

The security of a KDF depends on the input bitstring k which is sampled from a source of keying material ϕ. Formally, ϕ is an efficient algorithm that takes as input the security parameter 1^η and outputs the probability distribution tuple (k, α). In the tuple output by the source ϕ, k is the bitstring that will be input to the KDF and α is auxiliary knowledge about k which is known to the adversary.

The standard security definition for a KDF demands that the output bitstring is indistinguishable from a random bitstring of the same length. The definition refers to an experiment that is played between an adversary $\mathcal{B}$ and an oracle $\mathcal{O}_{\mathcal{K}}$ that will derive keys for adaptively chosen context and length queries. The secure KDF experiment is defined as follows:

(t,q,ε)-Secure-KDF$_{\mathcal{O}_{\mathcal{K}}}(\eta, q, \mathcal{B})$

1) The oracle $\mathcal{O}_{\mathcal{K}}$ simulates the keying algorithm ϕ which generates the probability distribution tuple (k, α) and then provides the adversary $\mathcal{B}$ with the auxiliary knowledge α.
2) For $i = 1, \ldots, q' \leq q$, $\mathcal{B}$ adaptively submits chosen context and length queries to the key derivation oracle $\mathcal{O}_{\mathcal{K}}$ and learns the corresponding KDF output $k'_i = \mathcal{O}_{\mathcal{K}}(k, x_i, l_i)$.
3) Challenge: The adversary $\mathcal{B}$ chooses a context and length query (x, l) such that $x \notin \{x_1, \ldots, x_{q'}\}$. In other words the context x has not previously been submitted to $\mathcal{O}_{\mathcal{K}}$.
4) A bit $b \in \{0, 1\}$ is chosen at random. If $b = 0$ then $\mathcal{O}_{\mathcal{K}}$ provides $\mathcal{B}$ with the KDF output $k' = \mathcal{O}_{\mathcal{K}}(k, x, l)$, otherwise $\mathcal{O}_{\mathcal{K}}$ provides a random bitstring $k' = \{0, 1\}^l$ of length l bits.
5) $\mathcal{B}$ may repeat Step 2, subject to the total number of queries remaining less than q and the context not being equal to the challenge context x.
6) The adversary $\mathcal{B}$ outputs a bit $b' \in \{0, 1\}$. $\mathcal{B}$ wins the game if $b' = b$.

Definition 2 (Secure KDF)**.** A KDF $\mathcal{K}$ is said to be (t, q, ε)-secure with respect to a source of keying material ϕ, if for all efficient adversaries $\mathcal{B}$ that run in time t and make at most q queries, the probability of $\mathcal{B}$ winning the **(t,q,ε)-Secure-KDF** experiment is less than $1/2 + \varepsilon$.

III. System and Adversarial Model

This section describes the ETSI V2X system model, the broadcast message format and the threat model under which we analyse the scheme.

A. V2X System Model

In this paper, we follow the ETSI ITS model for V2X [5] shown in Figure 1. ITS systems (vehicles) are equipped with an onboard unit (OBU). Each OBU contains a trusted hardware element (TE), most likely a smart card, which provides secure key storage and can perform some basic cryptographic operations. The PKI environment comprises one or more of both an enrolment authority (EA) and an authorisation authority (AA).

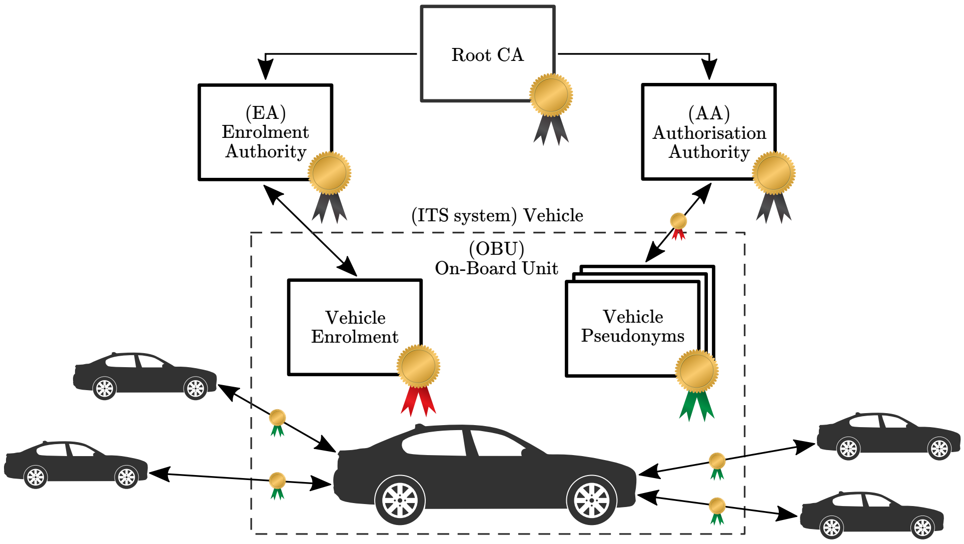

Fig. 1. ETSI Standard V2X PKI architecture [5].

The role of an EA is the long-term identification and authentication of ITS systems. An AA authorises pseudonymised ITS systems to use a particular application or service. The separation of EA and AA functionality is intended to facilitate user privacy [39].

B. V2X Broadcast Message Format

In the ETSI model the messages which are exchanged between vehicles to create and maintain situational awareness are termed Cooperative Awareness Messages (CAM) [37]. CAM are structured according to the ETSI CAM security profile [40] of the IEEE WAVE standard [41]. The general structure of a CAM message is shown in Figure 2.

C. Threat Model

For our formalisation of V2X privacy we assume that the vehicle OBU is an honest device which will correctly execute the IFAL algorithms and which has access to a clock source which is loosely synchronised with other vehicle OBUs. This assumption is necessary because an untrustworthy OBU could send arbitrary privacy-compromising data to nearby listeners (e.g. a unique value could be inserted into every message). If the clock source were adversarially controlled then a vehicle could be tricked into signing its messages using a specific or previously-seen pseudonym certificate, undermining the privacy provided by periodic pseudonym change. This is the same assumption that is made when modelling the privacy properties of Direct Anonymous Attestation [42].

For our formalisation of both security and privacy we assume that the vehicle TE is a trusted and suitably audited secure hardware element which can generate an ECDSA key-pair, securely store the private key and will correctly execute the IFAL message signing algorithm. Any mass market smart-card such as the NXP SmartMX or JCOP Java cards would make a suitable TE. We assume that the EA and AA are honest-but-curious [36] adversaries that will correctly execute the IFAL protocol, which do not collude, but that may opportunistically attempt to learn more than is specified by the protocol. All of this is directly inherited from the ETSI ITS standard.

Our formalisation of V2X security holds under the weaker assumption that the OBU may be malicious, although denial-of-service is a possibility in this setting. IFAL ensures that V2X security is retained provided the TE is uncompromised.

We focus our analysis on the cryptographic properties of IFAL as a secure and privacy conscious V2X scheme, and therefore we assume that the metadata of the network and the lower communication layers cannot be used to identify vehicles. This is a realistic assumption when considering that PKI enrolment and certificate file issuance in our scheme is a one-time process, and is likely to take place at manufacture time. The delivery of IFAL activation codes can be highly infrequent and may even take place offline, for example during vehicle servicing.

ITS Header	Basic Container	HF Container	LF Container (Conditional)	Special Vehicle Container (Conditional)

Fig. 2. General structure of a CAM [37].

IV. Requirements

This section defines the standard requirements for ETSI compatible V2X security architecture. We denote the security, privacy and functional requirements by SR, PR and FR, respectively. We denote an arbitrary signed message (m, σ_i), where σ_i is a valid digital signature on message m with respect to a pseudonym certificate ρ_i. We use the term 'canonical identity' to refer to the proper legal identity of the vehicle occupant or owner.

- SR1 - *Message authenticity*. A recipient of a V2X signed message (m, σ_i) and its corresponding pseudonym certificate ρ_i must be certain of its integrity and (pseudonymous) origin.
- PR1 - *Vehicle pseudonymity*. A signed message (m, σ_i) and its pseudonym certificate ρ_i must not reveal the canonical identity of the vehicle owner.
- PR2 - *Vehicle accountability*. Optionally, a suitable authority should be able to resolve a signed message (m, σ_i) and its pseudonym certificate ρ_i to a canonical identity.
- PR3 - *Pseudonym unlinkability*. Given a pseudonym certificate ρ_i, an adversary should learn nothing about a distinct pseudonym certificate ρ_j which it did not know before learning ρ_i.
- PR4 - *Corrupt CA tolerance*. The corruption of a single authority (i.e. either the EA or the AA) must not enable any number of signed messages $(m, \sigma_0), \ldots, (m', \sigma_j)$ or the pseudonym certificates which authenticate them $\rho_0, \ldots, \rho_j$ to be linked to any canonical vehicle identity. See Section V-C1 for our discussion of the limits on achievable privacy in V2X.
- FR1 - *Limited and intermittent vehicle connectivity*. A V2X scheme must support vehicles that have limited bandwidth and which suffer from intermittent connectivity to centralised services. It is likely that there will be a large number of retrofitted connected vehicles during early deployment.
- FR2 - *Limited vehicle resources*. A V2X scheme must be designed with respect for the limited processing and storage capabilities of the vehicle OBU. The standard benchmark in the literature is that a vehicle must be able to cryptographically verify as many as 1000 messages per second [43]. In addition, vehicles are expected to generate and sign 10 messages per second, and must not require excessive storage space for certificates.
- FR3 - *Sybil attack resistance*. A V2X scheme must resist attacks which depend upon creating large numbers of adversarially concocted pseudonymous identities.
- FR4 - *PKI removal of misbehaving vehicles*. A V2X scheme must be able to remove misbehaving vehicles. Vehicle removal should be possible using either the canonical identity or a pseudonym certificate sent by the vehicle.
- FR5 - *ETSI compliant*. The scheme must be compatible with the ETSI ITS security architecture [44]. This ensures that a scheme is practical, both in terms of European interoperability and meeting the performance requirements (i.e. those determined by PRESERVE [43]) on constrained vehicle hardware).

V. V2X Formal Model

This section describes our formalisation of the ETSI V2X system model and we formalise the terms 'secure V2X' and 'privacy conscious V2X'.

A. V2X Scheme

Definition 3. (V2X scheme). A V2X scheme Π comprises the following quartet of efficient algorithms and protocols:

- An algorithm `CreatePKI` that outputs the public and private PKI parameters $(\mathsf{PP}, \mathsf{SP})$ which are sets that include the public and private signing keys belonging to each root CA, EA and AA, respectively. In addition, the public parameters PP also includes the certificates ρ_{EA} and ρ_{AA} that authorise the EA and the AA, respectively, in relation to the root public key P_{RCA}.
- An algorithm `CreateVehicle` which outputs the public key pairs of a vehicle OBU $(k_{\text{OBU}}, P_{\text{OBU}})$ and the associated TE $(k_{\text{TE}}, P_{\text{TE}})$.
- An interactive protocol `EnrolVehicle` that is run between the EA and a vehicle.
- An interactive protocol `AuthoriseVehicle` that is run between the AA and a vehicle.

B. V2X Security

The main security requirement for a V2X scheme is message authentication. In this section, we capture this requirement by formalising the term "secure V2X" scheme in relation to the authentication experiment **Auth-V2X**. To improve the completeness of our definition, we overload the standard digital signature verification algorithm $\mathcal{V}$ from Section II-B as follows. In the authentication experiment **Auth-V2X**, the verification algorithm $\mathcal{V}$ takes as input the full certificate chain that authorises the verification key P. Specifically, $\mathcal{V}$ takes as input the V2X scheme root certificate public key P_{RCA}, the AA certificate ρ_{AA}, the pseudonym certificate ρ, the message m and the signature σ. The modified verification algorithm $\mathcal{V}$ returns true only if:

1) The tuple (m, σ) is a valid digital signature with respect to the definition of a secure signature scheme in Section II-B. In other words, where P is the verification key in the pseudonym certificate ρ, $\mathcal{V}(P, m, \sigma)$.
2) There is a valid certificate chain from the pseudonym certificate ρ to the root certificate public key P_{RCA}. e.g., $\mathcal{V}(P_{\text{RCA}}, \rho_{\text{AA}}, \sigma_{\rho_{\text{AA}}}) = 1$ and $\mathcal{V}(P_{\rho_{\text{AA}}}, \rho, \sigma_\rho) = 1$.

The authentication experiment is played between an adversary $\mathcal{C}$ and a V2X scheme oracle $\mathcal{O}_\Pi$ that simulates a number of vehicles. The experiment is as follows:

Auth-V2X$_{\mathcal{O}_\Pi}(1^\eta, \mathcal{C})$

1) The V2X scheme oracle $\mathcal{O}_\Pi$ takes as input the security parameter 1^η and simulates the `CreatePKI` algorithm which outputs the public and private PKI parameters $(\mathsf{PP}, \mathsf{SP})$ and also the `CreateVehicle` algorithm which creates N_V vehicles with identities $V_1, \ldots, V_{N_V}$. The oracle $\mathcal{O}_\Pi$ provides the adversary $\mathcal{C}$ with the public parameters $\mathsf{PP} = (P_{\text{RCA}}, P_{\text{EA}}, \rho_{\text{EA}}, P_{\text{AA}}, \rho_{\text{AA}})$.
2) Challenge: For an arbitrary polynomial duration of $\mathcal{C}$'s choosing, $\mathcal{O}_\Pi$ provides $\mathcal{C}$ with the message-signature-certificate triples (m, σ, ρ) that are sent by the vehicles $V_1, \ldots, V_{N_V}$. Afterwards, the adversary $\mathcal{C}$ outputs the triple of bitstrings $(m^\star, \sigma^\star, \rho^\star)$.

The adversary $\mathcal{C}$ is deemed successful and wins the **Auth-V2X** experiment only if:

1) The message $m^\star$ is different from any m provided by the V2X scheme oracle $\mathcal{O}_\Pi$.
2) The triple $(m^\star, \sigma^\star, \rho^\star)$ corresponds to a valid message-signature pair $(m^\star, \sigma^\star)$ with respect to the pseudonym certificate $\rho^\star$ and the certificate chain from ρ to P_{RCA} is valid. In other words, $\mathcal{V}(P_{\text{RCA}}, \rho_{\text{AA}}, \rho^\star, m^\star, \sigma^\star) = 1$.

Definition 4 (Secure V2X scheme)**.** We say that a V2X scheme Π is secure if for all efficient adversaries $\mathcal{C}$, the probability of $\mathcal{C}$ winning the **Auth-V2X** experiment is a negligible function of η.

C. V2X Privacy

In this section we formalise the privacy notions for a V2X scheme.

1) Achievable Privacy: We cannot cryptographically defend against the functional requirement that vehicles frequently broadcast unique positional and trajectory data to an audience bounded only by transmission distance [1]. Even 'perfectly unlinkable' V2X signatures which use a different pseudonym for each message are vulnerable to attacks which exploit the relationship between vehicle position and speed at different points in time [45], [46].

Instead, we consider separately the contents of broadcast messages and their cryptographic signatures. This allows us to quantify the privacy leakage of the cryptographic protocols of a V2X scheme in a way which is not dependent on either human behaviour or vendor specific implementation details. Defining V2X privacy in terms of cryptographic linkability, disentangled from the functional contents of CAM, captures the set of realistic adversaries who only have a partial overview of the whole environment. Such adversaries face periods of uncertainty in which a target vehicle is seemingly not broadcasting its location or trajectory. Provided there is sufficient noise in the form of other vehicles, an adversary becomes uncertain about reidentifying the target vehicle.

2) V2X Privacy: We capture the cryptographic linkability of a V2X scheme with the following experiment that is played between an adversary $\mathcal{D}$ and the "obscured" V2X scheme oracle $\mathcal{O}_{\not\Pi}$. The obscured oracle $\mathcal{O}_{\not\Pi}$ is like the V2X oracle $\mathcal{O}_\Pi$ from the **Auth-V2X** experiment in Section V-B. However, rather than directly providing the adversary with the messages that are broadcast by vehicles, $\mathcal{O}_{\not\Pi}$ sends messages that are chosen uniformly at random from a message distribution $\mathcal{M}$. Here we use the notion of a "vehicle reference" analogously to how pointers are used in computer programming languages, and our experiment is similar to the off-line RFID privacy model developed by Garcia et al. [47]. The **t-Priv-V2X** experiment is as follows:

t-Priv-V2X$_{\mathcal{O}_{\not\Pi}}(1^\eta, \mathcal{D})$

1) The obscured V2X scheme oracle $\mathcal{O}_{\not\Pi}$ takes as input the security parameter 1^η and simulates the `CreatePKI` algorithm which outputs the public and private PKI parameters $(\mathsf{PP}, \mathsf{SP})$ and also the `CreateVehicle` algorithm which creates N_V vehicles with references $V_1, \ldots, V_{N_V}$. The oracle $\mathcal{O}_{\not\Pi}$ provides the adversary $\mathcal{D}$ with the public parameters $\mathsf{PP} = (P_{\text{RCA}}, P_{\text{EA}}, \rho_{\text{EA}}, P_{\text{AA}}, \rho_{\text{AA}})$ and the vehicle references $V_1, \ldots, V_{N_V}$.
2) Challenge: After an arbitrary polynomial duration of $\mathcal{D}$'s choosing, during which $\mathcal{O}_{\not\Pi}$ provides $\mathcal{D}$ with all of the obscured message-signature-pseudonym triples (m, σ, ρ) that are sent by the vehicles $V_1, \ldots, V_{N_V}$, $\mathcal{D}$ chooses a target vehicle reference $V^\star \in \{V_1, \ldots, V_{N_V}\}$.
3) The oracle $\mathcal{O}_{\not\Pi}$ invalidates all of the original vehicle references $V_1, \ldots, V_{N_V}$, chooses a bit $b \in \{0, 1\}$ at random and then pauses for the polynomial duration t. During the time t, no messages from any of the vehicles $V_1, \ldots, V_{N_V}$ are sent to the adversary $\mathcal{D}$. After time t and if $b = 0$ then $\mathcal{O}_{\not\Pi}$ resumes simulating only the vehicle that had the reference $V^\star$, otherwise $\mathcal{O}_{\not\Pi}$ simulates a different vehicle chosen uniformly at random from $\{V_1, \ldots, V_{N_V}\} \setminus V^\star$.
4) After an arbitrary polynomial duration of $\mathcal{D}$'s choosing, during which $\mathcal{O}_{\not\Pi}$ provides $\mathcal{D}$ with all of the obscured message-signature-pseudonym triples (m, σ, ρ) that are sent by the remaining vehicle, $\mathcal{D}$ outputs the bit $b' \in \{0, 1\}$.

The adversary $\mathcal{D}$ is deemed successful and wins the **t-Priv-V2X** experiment if $b' = b$.

Definition 5 (Privacy conscious V2X)**.** A V2X scheme Π is said to be privacy conscious if for all efficient adversaries $\mathcal{D}$, the probability of $\mathcal{D}$ winning the **t-Priv-V2X** experiment is less than $1/2 + \epsilon$.

VI. IFAL

This section presents the full design and specification of our IFAL V2X scheme. For simplicity and without loss of generality, we consider just one of each enrolment (EA), authorisation (AA) and root CAs. Furthermore, we only consider the most fundamental ITS service of basic CAM sending. The IFAL scheme straightforwardly scales to a wide range of ITS services, such as Electronic Traffic Pricing [48], and to a larger ecosystem of certificate authorities.

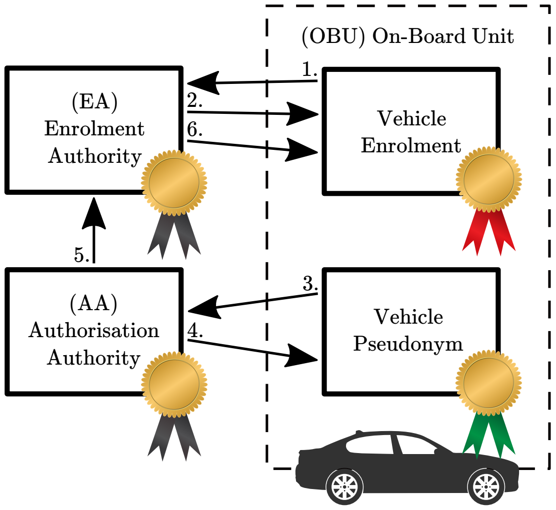

Fig. 3. Simplified IFAL PKI model.
1. The vehicle owner registers ID and public key value with the EA.
2. The EA provides the vehicle with an enrolment certificate and a unique uid value.
3. The vehicle provides the enrolment certificate, its uid and an activation code distribution channel specification to the AA.
4. The AA provides the vehicle with a pseudonym certificate file.
5. The AA periodically sends activation codes for all entitled vehicles to the EA.
6. The EA distributes activation codes by relating the uid to a vehicle identity and a distribution channel specification.

The differentiating approach of IFAL is to pre-issue vehicles with a lifetime supply of short-lived pseudonym certificates which can only be used after receiving an activation code. Each activation code allows a specific vehicle to, in essence, derive the pseudonym private keys for one epoch of pseudonym certificates. Since all cars sold in the EU are legally required since April 2018 to incorporate the 'eCall' emergency call system which equips each vehicle with a mobile SIM card, IFAL runs on existing infrastructure. Certificate pre-issuance enables IFAL to support vehicles which do not have always-on internet connections. Indeed, each activation code can be represented as a 28-character alphanumeric string, comprising a 128 bit symmetric key-factor and an additional 40 bit epoch and certificate file identifier. IFAL activation codes are therefore easily sent using an SMS, or may even be entered manually during a service interval. See Section VIII for a more thorough analysis of the connectivity and bandwidth reduction offered by the IFAL scheme.

IFAL removes the need for CRL as misbehaving vehicles are simply denied the activation codes which are necessary to derive the keys to future pseudonym certificates. The scheme is flexible with regards to trading between vehicle connectivity requirements and the maximum time period of vehicle misbehaviour following revocation. Small CRL could remain part of the scheme and would enable sufficiently connected vehicles and roadside equipment to be almost entirely protected from misbehaving entities.

IFAL runs on existing infrastructure and one fixed-size IFAL activation code can correspond to an arbitrary number of different pseudonym certificates. This is superior to using time-limited certificates, in which it is necessary to trade bandwidth (each certificate has a fixed size) for privacy - the time-limit of each certificate. Using the ETSI recommendation of 5 minutes per certificate and an optimistic 1024-bit certificate size, one days worth of pseudonym certificates would require 288 KB or 308 SMS messages which in practice is the difference between a vehicle requiring a data subscription or not.

The IFAL scheme consists of three stages: initialisation, activation and usage. Briefly and as shown in Figure 3, the EA provides each vehicle with a signed long-term enrolment credential and an associated uid. The uid is shared between the EA and the AA as a pseudonymous reference to the vehicle. Vehicles authenticate themselves to the AA by presenting a long-term enrolment credential and uid. The AA then provides batches of pseudonymous certificates which authorise a vehicle to send CAM.

Periodically, the AA sends new activation codes to the EA. The EA sends the activation codes to the vehicle using a pre-arranged channel (e.g. SMS).

A. IFAL Preliminaries

IFAL requires one or more trust anchors to be in place before the initialisation protocol is run. Specifically, IFAL requires a root CA and its signature on the EA and AA public keys. Each vehicle OBU must be securely issued the root CA public key during manufacture. The root CA public key is used to verify the EA and the AA during the remainder of the scheme.

The ETSI ITS standard [40] prescribes the use of either NIST Curve P-256 [49] or BrainpoolP256r1 [50] as the scheme elliptic curve C. Both curves specify base points G of prime order n, where n is of length 256 bits. The parameters C, G and n are public values which we do not explicitly pass as input to the algorithms which utilise them.

IFAL requires a hash function, a public key encryption scheme and a symmetric key encryption scheme for which, in accordance with the ETSI ITS standard, we specify SHA-256 [51], Elliptic Curve Integrated Encryption Scheme (ECIES) [52] and the NIST SP 800-108 AES CMAC pseudorandom function [53] respectively.

1) IFAL KDF definitions: IFAL makes use of two secure and standards-conformant KDFs which we denote $\mathcal{K}_1$ and $\mathcal{K}_2$. We define both $\mathcal{K}_1$ and $\mathcal{K}_2$ as NIST SP 800-108 key derivation functions [54] in counter mode, using cipher-based message authentication code (CMAC) [53] as the pseudorandom function. The length of derived keys for both $\mathcal{K}_1$ and $\mathcal{K}_2$ is 256 bits. Both $\mathcal{K}_1$ and $\mathcal{K}_2$ output elements in $Z_n \setminus \{0\}$ using any suitable technique [55].

$\mathcal{K}_2$ has the additional property of being a symmetric key encryption function. $\mathbb{E} = (E, D) = (\mathcal{K}_2, \mathcal{K}_2^{-1})$ such that for a key k, and a fixed-length derivation bitstring D , where $|D| \leq$256 bits, the property $\mathcal{K}_2^{-1}(k, \mathcal{K}_2(k, D)) = D$ holds.

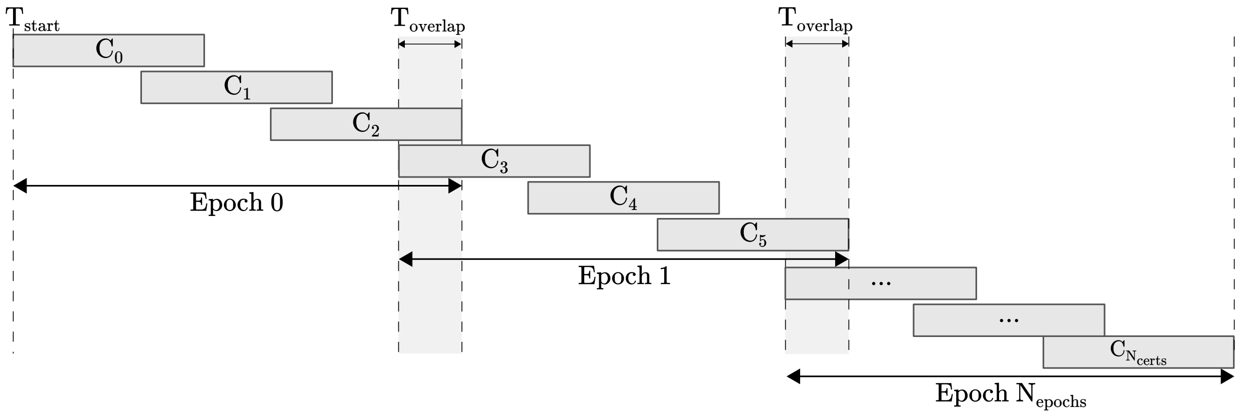

Fig. 4. IFAL policy parameters

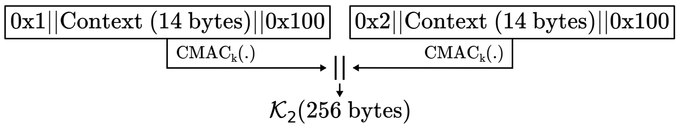

Fig. 6. $\mathcal{K}_2$ NIST SP 800-108 KDF construction

2) Policy Files: IFAL *Policy* files define the security parameters of the scheme as illustrated in Figure 4. A policy file specifies the pseudonym certificate validity period T_{period}, the pseudonym overlap period T_{overlap} which defines the requirements for time synchronisation between vehicles, the number of pseudonyms per certificate file N_{certs}, the number of epochs which divide the certificate file N_{epochs} and an *encoding* which specifies the expected format. The minimum certificate validity period is derived by subtracting the overlap period from the total validity period: $T_{\text{minimum}} = T_{\text{period}} - T_{\text{overlap}}$.

3) Certificate Files: A *certificate file* comprises a digest of the policy file, the valid-from time T_{start}, a transport key k_T and the list of signed certificates $C_0, \ldots, C_{N_{\text{certs}}}$. The transport key k_T is retained by the AA and is used to encrypt the activation keys which are transmitted to the vehicle via the EA.

4) Auxiliary Algorithms: IFAL requires two auxiliary algorithms which we now define.

- The `CreateMetadata` algorithm takes as input the IFAL policy file and returns the metadata which is put at the beginning of each certificate file. The metadata is a tuple which comprises the first certificate validity time T_{start}, a hash of the policy file, the transport key encrypted using the vehicle OBE public key $\texttt{ENC}(P_{\text{OBE}}, k_T)$ and a certificate file encoding specification.
- The `GetCertValidity` algorithm takes as input a certificate index i, a policy file and a certificate file start time T_{start}, and returns a tuple containing the start and end validity time of certificate i in the certificate file.

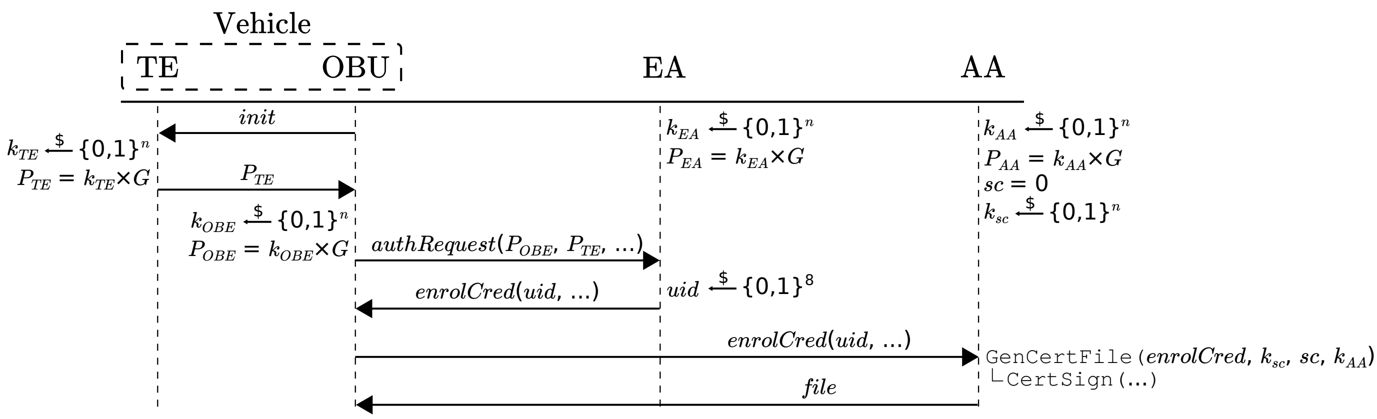

Fig. 5. IFAL initialisation protocol

B. IFAL Initialisation Protocol

The first stage of the IFAL scheme is the initialisation protocol, shown in Figure 5, during which a vehicle becomes enrolled in the scheme for the first time.

The vehicle OBU is installed with a policy file and a root certificate. The EA generates a public key pair $(k_{\text{EA}}, P_{\text{EA}})$ and the AA generates a public key pair $(k_{\text{AA}}, P_{\text{AA}})$, a signature counter symmetric key k_{sc} and a signature counter sc which is initialised to zero. The vehicle OBU generates a public key pair $(k_{\text{OBU}}, P_{\text{OBU}})$ and then initialises the TE, which generates a public key pair $(k_{\text{TE}}, P_{\text{TE}})$. The TE returns its public key to the OBU. The OBU composes the two vehicle public keys $P_{\text{OBU}}, P_{\text{TE}}$, the policy file, and an activation code channel specification into an $authRequest$ which is signed and then sent to the EA.

The EA receives the authRequest, verifies the signature, and awaits out-of-band documentation which asserts the vehicle registrant. The EA role is most naturally assumed by an existing national vehicle registration agency. Next, the EA generates a unique vehicle uid which is used as a pseudonymous vehicle reference between the EA and AA. The EA composes the authRequest and the uid into an enrolment credential $enrolCred$ which is signed, encrypted using the OBU public key P_{OBU} and then returned to the vehicle.

Finally, the OBU requests the certificate *file* from the AA by submitting its enrolment credential. The AA calls the `GenCertFile` algorithm (Algorithm 1) which creates the certificate file and the associated activation codes. The pseudonym activation codes are linked to the vehicle uid and retained by the AA. The certificate file is returned to the requesting vehicle which verifies that the file was crafted in accordance with the policy.

1) Initialisation Algorithms: During the IFAL initialisation protocol, the AA creates a certificate file by calling the `GenCertFile` algorithm. Each pseudonym certificate in the certificate file is issued by calling the `CertSign` algorithm (See Algorithm 2).

Algorithm 1: `GenCertFile`

input: authRequest, k_{sc}, sc, k_{AA}
Create new record for uid
for $j \leftarrow 0$ **to** $N_{epochs-1}$ **do**
  $k_j \xleftarrow{\$} \{0,1\}^n$
Add $k_0, \ldots, k_{N_{\text{epochs}-1}}$ to the record for uid
Generate new file
header = `CreateMetadata`(*policy*)
Write header to file
for $i \leftarrow 0$ **to** N_{certs} **do**
  $j = i/N_{\text{epochs}}$
  validity = `GetCertValidity`(*i, policy*)
  $P_i = \mathcal{K}_1(k_j, i) \times P_{\text{TE}}$
  content = validity $\|$ P_i
  signature = `CertSign`(*content, uid, k_{sc}, sc, k_{AA}*)
  certificate = content $\|$ signature
  Write certificate to file
return *file*

The `GenCertFile` algorithm takes as input the authRequest from the vehicle, the signature counter key k_{sc}, the signature counter sc and the AA private key k_{AA}. The authRequest contains the IFAL policy file and the vehicle public keys $(P_{\text{OBU}}, P_{\text{TE}})$. The policy file specifies the number of pseudonym certificates N_{certs} and the number of epochs N_{epochs} which are used by the algorithm. The algorithm returns an IFAL certificate file which contains a batch of pseudonym certificates and the metadata necessary to use them. The certificate file is encrypted using the vehicle OBU public key P_{OBU}.

Algorithm 2: `CertSign`

input: pseudonym, uid, k_{sc}, sc, k_{AA}
1 $sc = sc + 1$
2 **if** $sc = (2^{|sc|} - 1)$ **then**
3   $k_{\text{AA}} \xleftarrow{\$} \{0,1\}^n$
4   $P_{\text{AA}} = k_{\text{AA}} \times G$
5   $k_{sc} \xleftarrow{\$} \{0,1\}^n$
6   $sc = 0$
7 $k = \mathcal{K}_2(k_{sc}, sc \parallel uid)$; $(x, y) = k \times G$
8 $r = x \ mod \ n$; $h =$`Hash`(*pseudonym*)
9 $s = k^{-1}(h + k_{\text{AA}} * r) \ mod \ n$
10 **if** $r = 0 \ OR \ s = 0$ **then**
11   goto line 1
12 **return** (r, s)

The `CertSign` algorithm returns a signed IFAL pseudonym certificate. The algorithm performs a variant of the deterministic ECDSA signature algorithm [56] in which the randomisation key k, which is usually a random bitstring, is derived by applying the secure KDF $\mathcal{K}_2$, such that $k = \mathcal{K}_2(k_{sc}, sc \parallel uid)$. The derived key k can be used by the AA to recover the uid from messages signed by a misbehaving vehicle.

The signature counter sc is incremented each time the `CertSign` algorithm is called so that each signature key and counter tuple (k_{sc}, sc) is unique. The algorithm also checks that sc has not reached its maximum value and, once reached, generates a new signature key k_{sc}, re-initialises sc to zero and generates a new public key pair $(k_{\text{AA}}, P_{\text{AA}})$.

C. IFAL Activation Protocol

The IFAL activation protocol is a periodic process in which the AA distributes new activation codes to authorised vehicles via the EA. Each activation code permits the vehicle to generate the set of pseudonym private keys which correspond to one epoch of certificates from the certificate file.

The activation protocol proceeds as shown in Figure 7. The AA maintains a database which relates the pseudonymous uid of each vehicle and the activation codes which were generated during the initialisation protocol. The AA iterates the database and sends each uid and the next corresponding *activationCode* to the EA. Separately, the EA maintains a database which links each uid with a canonical vehicle identity and an activationCode channel specification. The EA sends each new activationCode to the vehicle corresponding to the uid indicated by the AA. The activationCode channel can range from manual installation (e.g. during annual servicing) to ad-hoc over-the-air delivery, depending upon the connectivity of the vehicle. Each activationCode is only 128 bits in size and is therefore readily sent using an SMS message. The vehicle decrypts the activationCode using the transport key which was in the certificate file received from the AA during the initialisation protocol.

D. IFAL Usage Protocol

The IFAL usage protocol is run each time a vehicle signs a message. The protocol is comparable to the ECDSA algorithm, however the message digest is subject to an additional transformation process (similar to Chaum's blind signatures [57]) and the algorithm execution steps are shared between the vehicle TE and OBU. Specifically, the OBU computes the hash of the message and then applies a transformation function. The TE generates a signature on the transformed message hash which is returned to the OBU. The OBU applies a final transformation to the signature which completes the signature generation process.

Algorithm 3: `MessageSign`

input: $message$, t, T_{start}, T_{minimum}, N_{certs}
$i = (t - T_{\text{start}})/T_{\text{minimum}}$
epoch $= i/N_{\text{certs}}$
`/* If no` k_{epoch} `return error */`
$k_{\text{cert}} = \mathcal{K}_1(k_{\text{epoch}}, i)$
$h =$ `Hash`$(message)$
$h' = h * k_{\text{cert}}^{-1}\ mod\ n$
$(r, s) =$ `Sign`(h')
$s' = s * k_{\text{cert}}\ mod\ n$
return (r, s')

The vehicle OBU computes the IFAL signature on a message as follows (See Algorithm 3). Firstly the `MessageSign` algorithm identifies the epoch key k_{epoch} corresponding to the certificate which is valid at the time of sending the message. The `MessageSign` algorithm takes as input the unsigned message, the current vehicle time t, the certificate file start time T_{start}, the minimum certificate validity period T_{minimum} and the number of certificates N_{certs}.

Next, The pseudonym private key k_{cert} is derived by applying the $\mathcal{K}_1$ KDF to the certificate index value i using the epoch key k_{epoch}. The algorithm computes the hash digest h of the message, and then multiplies it by the inverse pseudonym private key k_{cert}^{-1} to yield the transformed message digest h'.

Algorithm 4: `Sign`

input: h', k_{TE}
1 $k \xleftarrow{\$} \mathbb{Z}_n \setminus \{0\}$
2 $(x, y) = k \times G$
3 $r = x\ mod\ n.$
4 $s = k^{-1}(h' + k_{\text{TE}} * r)\ mod\ n$
5 **if** $r = 0$ *OR* $s = 0$ **then**
6 | goto line 1
7 **return** (r, s)

The algorithm execution now passes to the vehicle TE which runs the `Sign` algorithm (Algorithm 4). The `Sign` algorithm takes as input the transformed message digest h' and the TE private key k_{TE}, and returns the ECDSA signature (r, s) on h'.

The vehicle OBU takes the TE signature (r, s) and transforms s by multiplying it by the pseudonym private key k_{cert} to yield $s' = k_{\text{cert}} * s$. The IFAL signature (r, s') is output by the `MessageSign` algorithm.

We show that the signature tuple (r, s') output by the `MessageSign` algorithm is a valid signature with respect to pseudonym public key P_i in the Appendix.

E. IFAL Removal of Misbehaving Vehicles

There are two different mechanisms by which vehicles can be removed from the IFAL PKI.

The first mechanism is that the EA receives a request to deactivate a vehicle based on its canonical identity. This could occur when a vehicle is taken off the road by its owner, or after a vehicle is 'written off' by an insurer following an accident. The EA uses the canonical vehicle registration information to look up the uid associated with the vehicle and then sends a removal request to the AA. The AA will no longer issue activation codes to the vehicle and so the vehicle will be unable to create valid message signatures after, at most, the duration of one certificate policy file epoch. The EA gate keeps re-enrolment depending upon the reasons for deactivation and based on existing regional vehicle registration laws.

The second mechanism is that the AA is notified, by a suitable authority, of pseudonym certificates belonging to

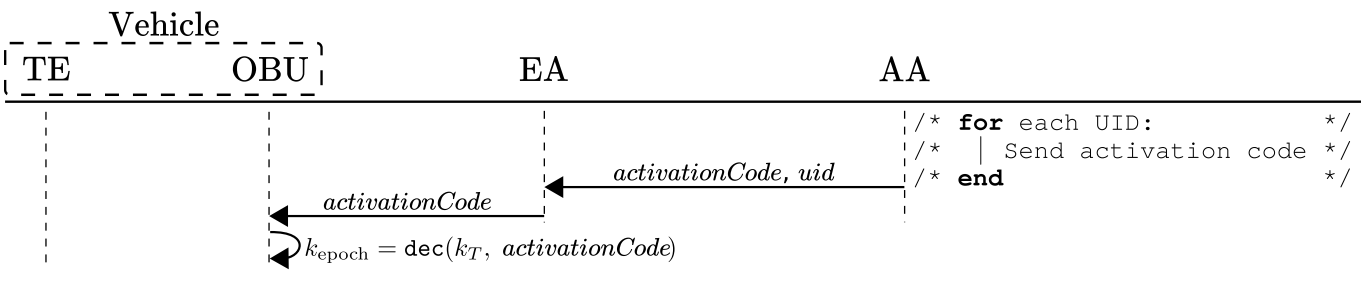

Fig. 7. IFAL activation protocol

a vehicle which has misbehaved. For example, the vehicle might have been involved in a hit-and-run accident. The pseudonym certificate will be of the form (r, s), where $(r, s) = (x \ mod \ n, \ k^{-1}(h + k_{AA} * r) \ mod \ n)$. This can be re-written in terms of k such that $k = s^{-1}(h + k_{AA} * r) \ mod \ n$. As k was generated by the invertible KDF $\mathcal{K}_2$, the AA can use $\mathcal{K}_2^{-1}(k_{sc}, k) = sc \parallel uid$ to recover the uid of the vehicle which has sent the message. The AA will no longer issue activation codes to this uid, and can also share the uid with the EA so that the canonical vehicle registration information can be linked to the incident.

VII. Security and Privacy of IFAL

A. IFAL Security Proof

This section shows that IFAL is a secure V2X scheme with respect to Definition 4. In particular, we reduce the security of IFAL to the unforgeability of the underlying signature scheme.

Theorem 1. *Let Σ be a secure signature scheme with respect to Definition 1, then IFAL is a secure V2X scheme with respect to Definition 4.*

Proof. Let us assume for contradiction that IFAL is not a secure signature scheme. In relation to the **Auth-V2X** experiment this means that there is an adversary $\mathcal{C}$ who after being provided with the public parameters $\mathsf{PP} = (P_{\text{RCA}}, P_{\text{EA}}, \rho_{\text{EA}}, P_{\text{AA}}, \rho_{\text{AA}})$ and all of the message-signature-certificate triples (m, σ, ρ) which are sent by N_V vehicles during an arbitrary period of observation, manages to craft a triple $(m^\star, \sigma^\star, \rho^\star)$ such that $m^\star$ is unique from any m sent by any vehicle and $\mathcal{V}(P_{\text{RCA}}, \rho_{\text{AA}}, \rho^\star, m^\star, \sigma^\star) = 1$.

We show how to use such an adversary $\mathcal{C}$ to break the security of the underlying signature scheme. Specifically, we construct an adversary $\mathcal{A}$ that uses $\mathcal{C}$ to win the **EUF-CMA** experiment. $\mathcal{A}$ simulates the full IFAL PKI environment including the initialisation, activation and usage protocols as specified in Section VI. $\mathcal{A}$ generates the public and private PKI parameters $(\mathsf{PP}, \mathsf{SP})$. The public parameters $\mathsf{PP} = (P_{\text{RCA}}, P_{\text{EA}}, \rho_{\text{EA}}, P_{\text{AA}}, \rho_{\text{AA}})$ include the root public key and the public keys and certificates of the EA and the AA. The private parameters $\mathsf{SP} = (k_{\text{RCA}}, k_{\text{EA}}, k_{AA}, k_{\mathsf{sc}}, \mathsf{sc})$ include the private keys of the root CA and the EA as well as the private key, secure counter key and secure counter of the AA.

To begin, the adversary $\mathcal{A}$ simulates N_V vehicles by first creating the corresponding OBU and TE public key pairs $(k_{\text{OBU}}, P_{\text{OBU}})$ and $(k_{\text{TE}}, P_{\text{TE}})$, respectively. For each simulated vehicle, $\mathcal{A}$ runs the initialisation and activation protocols so that the certificate file is generated and the pseudonym keys are available. $\mathcal{A}$ chooses the target pseudonym validity period $e^\star$ and the target vehicle $V^\star \in \{V_1, \ldots, V_{N_V}\}$. When emulating $V^\star$ during the target epoch $e^\star$, rather than using the vehicle private keys $(k_{\text{OBU}}, k_{\text{TE}})$ and simulating the usage protocol, $\mathcal{A}$ will instead use the signing oracle $\mathcal{O}_{\mathcal{S}}$ from the **EUF-CMA** game. For all other vehicles $\mathcal{A}$ will simulate the usage protocol as usual.

After an arbitrary period of adversary $\mathcal{C}$'s choosing, during which $\mathcal{A}$ will simulate periodic message sending and provide $\mathcal{C}$ with the message-signature-certificate tuples (m, σ, ρ) sent by all N_V vehicles, $\mathcal{C}$ will terminate and output a triple of bitstrings $(m^\star, \sigma^\star, \rho^\star)$. By hypothesis, $m^\star$ is unique from any m sent by any vehicle and $\mathcal{V}(P_{\text{RCA}}, \rho_{\text{AA}}, \rho^\star, m^\star, \sigma^\star) = 1$. In other words, $(m^\star, \sigma^\star)$ is a valid message-signature tuple and there is a valid certificate chain from the root public key P_{RCA} to the pseudonym certificate $\rho^\star$.

Since IFAL is based on the ETSI V2X standards, the signed message $(m^\star, \sigma^\star)$ must be an IEEE WAVE based CAM crafted according to the ETSI CAM security profile [40]. In particular, $(m^\star, \sigma^\star)$ is a `IEEE1609dot2 SignedData` structure as shown in Figure 8 such that $m^\star$ is the triple (`hashID`, `tbsData`, `signer`) and $\sigma^\star$ is the `signature` element.

```
SignedData ::= SEQUENCE {
hashId HashAlgorithm,
tbsData ToBeSignedData,
signer SignerIdentifier,
signature Signature
}
```

Fig. 8. The `SignedData` specification from the IEEE 1609.2 standard [41].

```
SignerIdentifier ::= CHOICE {
digest  HashedId8,
certificate SequenceOfCertificate,
self  NULL,
...
}
```

Fig. 9. The `SignerIdentifier` specification from the IEEE 1609.2 standard [41].

In order to win the **EUF-CMA** experiment, the adversary $\mathcal{A}$ needs to output a signed message $(m^\star, \sigma^\star)$ such that:

1) The message $m^\star$ is different from all of the queries made by $\mathcal{A}$ to the oracle $\mathcal{O}_{\mathcal{S}}$.
2) The tuple $(m^\star, \sigma^\star)$ is a valid message-signature pair relative to the verification key $P^\star$ and therefore $\mathcal{V}(P^\star, m^\star, \sigma^\star)$.

Condition 1. holds because $m^\star$ was not queried to the oracle $\mathcal{O}_{\mathcal{S}}$. As the target vehicle $V^\star$ is chosen randomly by $\mathcal{A}$, the probability that C attacks $V^\star$ is $1/N_V$. Condition 2. holds because $(m^\star, \sigma^\star)$ is a valid message-signature tuple with respect to the certificate chain from P_{RCA} to $\rho^\star$. With respect to the CAM message structure in Figure 8, this also means that if the `SignerIdentifier` element shown in Figure 9 is a `digest` then the adversary $\mathcal{A}$ has previously received the corresponding certificate $\rho^\star$.

The advantage of the adversary $\mathcal{C}$ in winning the **Auth-V2X** experiment is therefore the probability that $\mathcal{C}$ attacks vehicle $V^\star$ multiplied by the advantage of $\mathcal{A}$ against the signature scheme. Since $\mathcal{C}$ may attack either the signature on the message during the certificate validity period $e^\star$, or the signature at any stage of the certification path, the advantage of $\mathcal{C}$ is further divided by the certification path length ℓ and the total number of pseudonym validity periods N_E over which $\mathcal{A}$ provides tuples (m, σ, ρ) to $\mathcal{C}$.

$$\mathsf{Adv}_{\mathcal{C}}^{\textbf{Auth-V2X}} = \frac{\mathsf{Adv}_{\mathcal{A}}^{\textbf{EUF-CMA}}(1^{\eta})}{\ell * N_V * N_E}$$

B. IFAL Privacy Proof

This section shows that IFAL is a privacy conscious V2X scheme with respect to Definition 5. We reduce the privacy of IFAL to the security of the underlying KDF scheme.

Informally, an adversary cannot link vehicle pseudonyms to a single source because all pseudonym public keys are the product of a random vehicle TE public key and an output from the secure KDF $\mathcal{K}_1$. To win the **t-Priv-V2X** experiment with a non-negligible probability, an adversary must be able to learn or know something that can differentiate pseudonyms sent from one vehicle from those sent by another. Since a secure KDF has the property that the output is indistinguishable from a random bitstring of the same length, and random bitstrings do not portend anything about future random bitstrings, no adversary can link different pseudonyms to a single source.

IFAL is a privacy conscious V2X scheme because a secure KDF is used to derive the pseudonym public key values that are issued to vehicles. In more detail, each pseudonym public key P_i is computed as the product of the vehicle TE public key k_{TE} and the output of the KDF $\mathcal{K}_1$ which is seeded with the epoch key k_j and the context i, $P_i = \mathcal{K}_1(k_j, i) \times P_{\text{TE}}$. Correspondingly, vehicles use an implicit KDF to derive the pseudonym private key that is required to sign messages that are valid with respect to P_i. We define the implicit pseudonym private key KDF as follows:

$$\mathcal{K}_{\text{pseudo}}(k_j, i) = \mathcal{K}_1(k_i, i) * k_{\text{TE}} \mod n$$

Theorem 2. *If $\mathcal{K}_1$ is a secure KDF with respect to Definition 2 then $\mathcal{K}_{pseudo}$ is also a secure KDF.*

By definition, the output of KDF $\mathcal{K}_1$ is indistinguishable from a random bitstring in the field $\mathbb{Z}_n^*$. Since the vehicle TE private key k_{TE} is a generated securely by tamper-resistant hardware and modular multiplication over a prime modulus n is uniformly distributed in $\mathbb{Z}_n^*$, $\mathcal{K}_{\text{pseudo}}$ is a secure KDF. Even if k_{TE} is generated non-uniformly, provided that it is in the field $\mathbb{Z}_n^*$ then $\mathcal{K}_{\text{pseudo}}$ is still a secure KDF

Theorem 3. *If $\mathcal{K}_{pseudo}$ is a secure KDF then IFAL is a privacy conscious V2X scheme with respect to Definition 5.*

From Theorem 2 it follows that every pseudonym private key k_{pseudo} that is used to sign CAM in IFAL is a random bitstring in the field $\mathbb{Z}_n^*$. Each corresponding pseudonym public key is computed by multiplying k_{pseudo} by the elliptic curve base point G. In other words, $P_i = k_{\text{pseudo}} \times G = k_i * k_{\text{TE}} \times G = \mathcal{K}_1(k_j, i) * k_{\text{TE}} \times G$. Multiplying a random bitstring by an ellpitic curve point does not yield a secure KDF because, on all standard curves, a curve point is highly-distinguishable from a random bitstring [58]. Instead, for our notion of a privacy conscious L2V, we analogously formulate that the pseudonym public key must be indistinguishable from a random point on the same curve. It therefore suffices that the pseudonym private key k_{pseudo} is output by a secure KDF.

Proof. Let us assume for contradiction that IFAL is not a privacy conscious V2X scheme. This means that there is an adversary $\mathcal{D}$ that manages with a non-negligible probability to win the **t-Priv-V2X** experiment. We build an adversary $\mathcal{B}$ that uses $\mathcal{D}$ to win the **(q,t,ε)-Secure-KDF** experiment and therefore breaks the security of the underlying KDF.

To begin, the adversary $\mathcal{B}$ simulates the full IFAL PKI environment including the protocols, algorithms and roles specified in Section VI. $\mathcal{B}$ simulates N_V vehicles by generating the appropriate public key pairs and then simulating the initialisation and activation protocols. $\mathcal{B}$ chooses a target epoch $e^\star$ and a target vehicle $V^\star$. For each vehicle $\mathcal{B}$ emulates message sending by periodically simulating the usage protocol to generate message-signature-pseudonym triples (m, σ, ρ). When simulating $V^\star$ during epoch $e^\star$, rather than using the KDF $\mathcal{K}_1$ to generate the pseudonym private key, $\mathcal{B}$ uses the key derivation oracle $\mathcal{O}_{\mathcal{K}}$ from the **(q,t,ε)-Secure-KDF** experiment. As in the **t-Priv-V2X** experiment, each vehicle message m is chosen uniformly at random from a message distribution $\mathcal{M}$. Adversary $\mathcal{B}$ provides $\mathcal{D}$ with a reference to each vehicle $V_1, \ldots, V_{N_V}$ and provides all of the vehicle broadcast message triples (m, σ, ρ).

After an arbitrary polynomial duration, adversary $\mathcal{D}$ will provide $\mathcal{B}$ with a target vehicle reference V_i. $\mathcal{B}$ will invalidate all of the vehicle references $V_1, \ldots, V_{N_V}$, choose a bit $b \in \{0, 1\}$ and then pauses for the duration t. If $b = 0$ then $\mathcal{B}$ resumes simulating vehicle V_i only, otherwise $\mathcal{B}$ resumes simulating a different vehicle chosen at random from $\{V_1, \ldots, V_{N_V}\} \setminus V_i$. Again $\mathcal{B}$ provides $\mathcal{D}$ with all of the message-signature-pseudonym triples (m, σ, ρ) that are sent by the remaining vehicle. Eventually $\mathcal{D}$ will terminate and output a bit $b' \in \{0, 1\}$.

By hypothesis, $b' = b$ with a probability significantly higher than $1/2 + \epsilon$. This means that adversary $\mathcal{D}$ has succeeded in distinguishing the pseudonyms sent by vehicle V_i from those of another and that one of the following must hold true

1) The silent period t is less than the minimum certificate validity period T_{minimum}. If $t \leq T_{\text{minimum}}$ then $V^\star$ will sign messages using a pseudonym certificate that has already been witnessed by $\mathcal{D}$. The adversary will be able to win the experiment with a probability of 1.
2) $\mathcal{D}$ found linkable information in the pseudonym certificates ρ that were sent by V_i.
3) The adversary $\mathcal{D}$ broke the security of the KDF $\mathcal{K}_1$ that generated V_i's pseudonym public keys and was able to distinguish the values from random points on the same curve. $\mathcal{D}$ must have chosen to attack the target vehicle so that $V_i = V^\star$ and during the target epoch $e^\star$.

Condition 1. only holds if $t <= T_{\text{minimum}}$ and Condition 2. does not hold provided that the pseudonym certificates are created in accordance with the ETSI standards and that they do not contain any linkable information. Condition 3. holds because, by hypothesis, $\mathcal{D}$ was able to output $b' = b$ with a probability significantly higher than $1/2 + \epsilon$. This means that

$\mathcal{D}$ was able to distinguish the pseudonym key values sent by V_i from those of any other vehicle $\{V_1, \ldots, V_{N_V}\} \setminus V_i$.

Where N_{periods} is the integer number of epoch periods that the experiment is run over and provided that $t > T_{\text{minimum}}$, the advantage of the adversary $\mathcal{D}$ in winning the **t-Priv-V2X** experiment is the probability that $\mathcal{D}$ attacks the vehicle $\mathcal{V}^\star$ during the target epoch $e^\star$ multiplied by the advantage of $\mathcal{B}$ against the KDF scheme.

$$\mathsf{Adv}_{\mathcal{D}}^{\textbf{t-Priv-V2X}} = \frac{\mathsf{Adv}_{\mathcal{B}}^{\textbf{(q,t,}\varepsilon\textbf{)-Secure-KDF}}(1^\eta)}{N_V * N_{\text{periods}}}$$

VIII. Evaluation and Performance

In this section we argue that the IFAL scheme we have presented in Section VI meets the ETSI V2X security architecture requirements from Section IV.

The security requirement of message authenticity (*SR1*) is satisfied because IFAL is a secure V2X as we have shown in Section VII-A.

There are four privacy requirements. Vehicle pseudonymity (*PR1*) is satisfied by the structure of ETSI CAM given in Figure 2, which does not reveal the canonical identity of the message sender, and by the fact that IFAL is a privacy conscious V2X scheme which we have shown in Section VII-B. Vehicle accountability (*PR2*) is satisfied because user pseudonymity can be revoked, as shown Section VI-E. We prove pseudonym unlinkability (*PR3*) in Section VII-B where we have shown that IFAL is a privacy conscious V2X scheme. Finally, IFAL satisfies the requirement for corrupt CA tolerance (*PR4*) because neither the EA nor the AA alone can determine the canonical identity of a vehicle from only captured V2X messages.

As specified in the relevant ETSI standards [59], the AA should be implemented using an HSM to execute the key generation, `GenCertFile` and `CertSign` algorithms. The HSM should generate the pseudonym certificates and the activation codes and encrypt them using the vehicle OBU public key P_{OBU} and the transport key k_T respectively. Access to the uid recovery operation outlined in Section VI-E should be controlled through a separate 'recovery HSM'. A dedicated misbehaviour authority (MA) [6] could be established and entrusted to operate the recovery HSM, thus ensuring that no single entity can revoke user pseudonymity.

There are four functional V2X scheme requirements. IFAL caters for limited and intermittent vehicle connectivity (*FR1*). Activation codes are only 128 bits in size and can therefore be represented as a 28-character alphanumeric string, including an additional 40 bit epoch and certificate file identifier. Activation codes can be be communicated over a wide range of different channels: one viable option is to use SMS which all new vehicles will be required to be equipped with (i.e. eCall), vehicles may even be entirely unconnected and activation codes manually installed during vehicle service intervals.

IFAL only requires limited OBU and TE resources (*FR2*). Signature verification, the most time critical operation, is unchanged from the standards, just one ECDSA verification. For signing, which has a modest 10 per second performance requirement, the computational complexity is only increased by one KDF function call and one modular inverse operation per pseudonym certificate every 5 minutes plus two modular multiplications per message. These small overheads can easily be accommodated within existing V2X hardware without a significant performance impact. A 5 year supply of IFAL certificates requires as little as 32.1 megabytes of vehicle OBU storage. We evaluate the IFAL certificate file creation and storage requirements more thoroughly in Section VIII-A.

IFAL is Sybil attack resistant (*FR3*) because, at most, only two IFAL pseudonym certificates are valid for a single vehicle at the same time (determined by T_{overlap}). Having two pseudonym certificates valid at the same time is optimal unless you are willing to accept strict time synchronization between the vehicles, and is much better than the SCMS C2C-CC pseudonym certificate pooling approach in which there are 20-40 simultaneously valid vehicle credentials which are changed weekly [24].

IFAL supports the PKI removal of misbehaving vehicles using either the vehicle canonical identity or a pseudonym certificate (*FR4*), as we have shown in Section VI-E. The parameters in an IFAL policy file exchanged during the initialisation protocol both determine the granularity with which misbehaving vehicles can be removed from the scheme and define the connectivity requirements for enrolled vehicles. A misbehaving vehicle can continue to misbehave for as long as the activation codes for future epochs are known. Equivalently, vehicles must be able to connect to an EA as often as they require new activation codes. These parameters therefore present a trade off between connectivity requirements for activation code issuance, certificate storage requirements, and the removal of misbehaving vehicles.

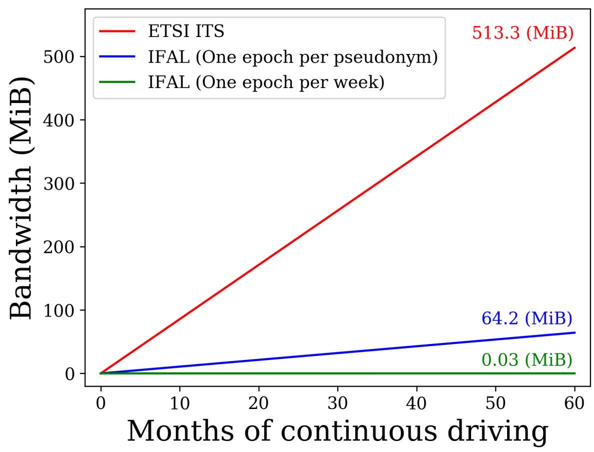

Fig. 10. IFAL vs. ETSI ITS: Cellular bandwidth requirements

IFAL is superior to the ETSI standard approach of using time-limited certificates because it is not necessary to compromise between the bandwidth required for transferring certificates and the privacy afforded by the time-limit of each certificate. Using the ETSI recommendation of 5 minutes per certificate and an optimistic 1024-bit certificate size, one days worth of pseudonym certificates would require at least 288 KB or 308 SMS messages of bandwidth. We compare the bandwidth requirements of the ETSI approach with IFAL in Figure 10.

In practice, IFAL will likely require less than a single text message worth of bandwidth per day and is the difference between a vehicle requiring a data subscription or not.

Finally, IFAL conforms to ETSI ITS standards and security architecture (*FR5*) as we have used the system model and the same cryptographic primitives.

A. Experimental Results

We have created a proof of concept reference implementation of IFAL in C++ based on the Crypto++ library and used our implementation to evaluate the practicality of our scheme.

Since signature verification on the vehicle is unchanged, namely a standard ECDSA verification operation, and we do not add significant computational complexity to message signing, we focused on the performance of the server-side `GenCertFile` and `CertSign` algorithms executed by the AA (See Algorithm 1 and 2 in Section VI-B).

We wrote an IFAL policy specifying a certificate file with a 5 year total duration, a 90 day epoch duration, a 5 minute pseudonym duration and a 2 minute overlap period. Using a standard desktop computer we were able to compute the certificate file containing 5 years of pseudonym certificates in 9.03 seconds on average. Our reference certificate file contains 525,600 pseudonym certificates and therefore requires at least $525,600 * 1024 \approx 64.2$ MB of storage on the vehicle. Additionally, the certificate file can be halved in size to just 32.1 MB if the vehicle OBE has sufficient resources to derive the pseudonym public keys as they are required.

We have made our reference implementation open source and freely available at https://github.com/hkscy/IFAL.

IX. Conclusion

In this paper we have presented the Issue First Activate Later (IFAL) V2X scheme which is a practical improvement upon the ETSI ITS standard V2X architecture.

We introduce a novel key diversification method that both avoids the need for certificate revocation and enables support for vehicles with limited and intermittent connectivity. The IFAL scheme pre-issues vehicles with a lifetime supply of pseudonym certificates during manufacture, divides the certificates into epochs and then periodically issues activation codes which enable a vehicle to derive pseudonym signatures during an epoch. By removing the need for CRL, IFAL offers improved verification latency over the previous proposals.

Activation codes are much smaller than the corresponding pseudonym certificates and therefore facilitate a much broader range of vehicle connectivities. Several activation codes fit within a single SMS message and may even be entered manually during vehicle servicing. Misbehaving vehicles are removed from the scheme by refusing to issue further activation codes and therefore denying vehicles the capability to sign messages.

We have shown that IFAL meets the ETSI ITS V2X architecture requirements, is provably secure and privacy conscious in a formal setting and has favourable performance in our reference implementation. IFAL is suitable for integration into the ETSI ITS standard.

Future research challenges include running simulations to determine optimal key management policies as well as symbolic protocol verification. Optimal pseudonym change strategies remain an open problem.

References

[1] D. Eckhoff and C. Sommer, "Marrying safety with privacy: A holistic solution for location privacy in VANETs," in *2016 IEEE Vehicular Networking Conference (VNC)*, Dec 2016, pp. 1–8.

[2] I. Symeonidis, A. Aly, M. A. Mustafa, B. Mennink, S. Dhooghe, and B. Preneel, "SePCAR: A Secure and Privacy-Enhancing Protocol for Car Access Provision," in *Computer Security – ESORICS 2017*, S. N. Foley, D. Gollmann, and E. Snekkenes, Eds. Cham: Springer International Publishing, 2017, pp. 475–493.

[3] A. Pham, I. Dacosta, G. Endignoux, J. R. T. Pastoriza, K. Huguenin, and J.-P. Hubaux, "Oride: A privacy-preserving yet accountable ride-hailing service," in *26th USENIX Security Symposium (USENIX Security 17)*. Vancouver, BC: USENIX Association, 2017, pp. 1235–1252.

[4] "Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)," October 2017.

[5] "ETSI TS 102 940. Intelligent Transportation Systems (ITS); Security; ITS communications security architecture and security management," European Telecommunications Standards Institute, Tech. Rep., November 2016.

[6] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for V2V communications," in *2013 IEEE Vehicular Networking Conference*, Dec 2013, pp. 1–8.

[7] "IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture," *IEEE Std 1609.0-2013*, March 2014.

[8] "Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport," *Official Journal of the European Union*, August 2010.

[9] "Insights on the regulatory activity for V2X with CTO Autotalks," Auto2x Ltd, Tech. Rep., November 2017.

[10] J. J. Haas, Y. C. Hu, and K. P. Laberteaux, "Efficient Certificate Revocation List Organization and Distribution," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 595–604, March 2011.

[11] T. Kosch, C. Schroth, M. Strassberger, and M. Bechler, *Automotive Internetworking*. John Wiley & Sons, Ltd, 2012, pp. 351–368.

[12] F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, E. Schoch, B. Wiedersheim, T. V. Thong, G. Calandriello, A. Held, A. Kung, and J. P. Hubaux, "Secure vehicular communication systems: implementation, performance, and research challenges," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 110–118, November 2008.

[13] "Workshop Summary," *C2C CC Security Workshop*, November 2006.

[14] "Intelligent transport systems – Cooperative ITS – Using V2I and I2V communications for applications related to signalized intersections," *ISO/TS 19091:2017*, pp. 1–211, March 2017.

[15] L. Apvrille, R. El Khayari, O. Henniger, Y. Roudier, H. Schweppe, H. Seudié, B. Weyl, and M. Wolf, "Secure automotive on-board electronics network architecture," in *FISITA 2010 world automotive congress, Budapest, Hungary*, vol. 8, 2010.

[16] M. Lagana, M. Feiri, M. Sall, M. Lange, A. Tomatis, and P. Papadimitratos, "Secure Communication in Vehicular Networks PRESERVE Demo," in *2012 IEEE Vehicular Networking Conference (VNC)*, November 2012.

[17] J. Walker, "Security Credential Management System Proof of Concept (Webinar)," September 2017.

[18] D. R. L. Brown, R. Gallant, and S. A. Vanstone, "Provably Secure Implicit Certificate Schemes," in *Financial Cryptography*, P. Syverson, Ed. Springer Berlin Heidelberg, 2002, pp. 156–165.

[19] S. A. Vanstone and M. Qu, "Implicit certificate scheme," Patent US6 792 530B1, September, 2004.

[20] M. Struik, "Implicit certificate verification," Patent US20 100 023 771A1, November, 2006.

[21] M. J. Campagna and M. Struik, "Self-signed implicit certificates," Patent US20 100 023 771A1, May, 2009.

[22] *Competition policy brief: Standard-essential patents*. European Commission, June 2014.

[23] "ETSI TR 103 415. Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management," European Telecommunications Standards Institute, Tech. Rep., April 2018.

[24] N. Bißmeyer, H. Stübing, E. Schoch, S. Götz, J. P. Stotz, and B. Lonc, "A generic public key infrastructure for securing Car-to-X communication," in *18th ITS World Congress, Orlando, USA*, vol. 14, 2011.

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

[26] L. Huang, H. Yamane, K. Matsuura, and K. Sezaki, "Towards modeling wireless location privacy," in *Privacy Enhancing Technologies*, G. Danezis and D. Martin, Eds. Springer, 2006, pp. 59–77.

[27] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," in *Embedded Security in Cars (ESCAR)*, 2005.

[28] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, 2007.

[29] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46–55, Jan. 2003.

[30] D. Förster, H. Löhr, J. Zibuschka, and F. Kargl, "Rewire – revocation without resolution: A privacy-friendly revocation mechanism for vehicular ad-hoc networks," in *Trust and Trustworthy Computing*, M. Conti, M. Schunter, and I. Askoxylakis, Eds. Cham: Springer International Publishing, 2015, pp. 193–208.

[31] J. Whitefield, L. Chen, F. Kargl, S. S. Andrew Paverd, H. Treharne, and S. Wesemeyer, "Formal Analysis of V2X Revocation Protocols," 2017.

[32] D. Förster, F. Kargl, and H. Löhr, "PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks," *Ad Hoc Networks*, vol. 37, pp. 122 – 132, 2016, special Issue on Advances in Vehicular Networks.

[33] J. Whitefield, L. Chen, T. Giannetsos, S. Schneider, and H. Treharne, "Privacy-enhanced capabilities for vanets using direct anonymous attestation," in *2017 IEEE Vehicular Networking Conference (VNC)*, November 2017, pp. 123–130.

[34] J. R. Douceur, "The sybil attack," in *Peer-to-Peer Systems*, P. Druschel, F. Kaashoek, and A. Rowstron, Eds. Springer, 2002, pp. 251–260.

[35] H. Krawczyk, "Cryptographic Extraction and Key Derivation: The HKDF Scheme," in *Advances in Cryptology – CRYPTO 2010*, T. Rabin, Ed. Springer Berlin Heidelberg, 2010, pp. 631–648.

[36] O. Goldreich, *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge University Press, 2011.

[37] "ETSI TS 302 637-2. Intelligent Transportation Systems (ITS); Security; Part 2: Specification of Cooperative Awareness Basic Service," European Telecommunications Standards Institute, Tech. Rep., September 2014.

[38] S. Goldwasser, S. Micali, and R. L. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen-message Attacks," *SIAM J. Comput.*, vol. 17, no. 2, pp. 281–308, Apr. 1988.

[39] "ETSI TS 102 731. Intelligent Transport Systems (ITS); Security; Security Services and Architecture," European Telecommunications Standards Institute, Tech. Rep., September 2010.

[40] "ETSI TS 103 097. Intelligent Transport Systems (ITS); Security; Security header and certificate formats," European Telecommunications Standards Institute, Tech. Rep., October 2017.

[41] "IEEE Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages," IEEE Vehicular Technology Society, Tech. Rep., January 2016.

[42] J. Camenisch, M. Drijvers, and A. Lehmann, "Anonymous attestation with subverted tpms," in *Advances in Cryptology – CRYPTO 2017*, J. Katz and H. Shacham, Eds. Cham: Springer International Publishing, 2017, pp. 427–461.

[43] "Security Requirements of Vehicle Security Architecture," PREparing SEcuRe VEhicle-to-X Communication Systems (PRESERVE), Tech. Rep., July 2011.

[44] "Intelligent Transport Systems (ITS); Communications Architecture," *ETSI EN 302 665*, September 2010.

[45] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *IEEE Wireless Communications and Networking Conference, 2005*, vol. 2, March 2005, pp. 1187–1192.

[46] N. Bißmeyer, S. Mauthofer, K. M. Bayarou, and F. Kargl, "Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters," in *2012 IEEE Vehicular Networking Conference (VNC)*, Nov 2012, pp. 78–85.

[47] F. D. Garcia and P. van Rossum, "Modeling privacy for off-line rfid systems," in *Smart Card Research and Advanced Application*, D. Gollmann, J.-L. Lanet, and J. Iguchi-Cartigny, Eds. Springer Berlin Heidelberg, 2010, pp. 194–208.

[48] F. D. Garcia, E. R. Verheul, and B. Jacobs, "Cell-based privacy-friendly roadpricing," *Computers & Mathematics with Applications (CAMWA)*, vol. 65, no. 5, pp. 774–785, 2013.

[49] "Digital Signature Standard (DSS) (FIPS 186-4)." National Institute of Standards and Technology, Tech. Rep., July 2013.

[50] M. Lochter and J. Merkle, "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation," Tech. Rep., March 2010.

[51] "Publication 180-4: Secure Hash Standard (SHS)," National Institute of Standards and Technology, Tech. Rep., August 2015.

[52] "IEEE Standard Specifications for Public-Key Cryptography - Amendment 1: Additional Techniques," *IEEE Std 1363a-2004 (Amendment to IEEE Std 1363-2000)*, pp. 1–167, Sept 2004.

[53] "Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication," National Institute of Standards and Technology, Tech. Rep., June 2016.

[54] "Special Publication 800-108. Recommendation for Key Derivation Using Pseudorandom Functions (Revised)," National Institute of Standards & Technology, Tech. Rep., 2009.

[55] "BSI TR-03111 Elliptic Curve Cryptography," Bundesamt für Sicherheit in der Informationstechnik, Tech. Rep., June 2012.

[56] T. Pornin, "Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)," Tech. Rep., August 2013.

[57] D. Chaum, "Blind signatures for untraceable payments," in *Advances in cryptology*. Springer, 1983, pp. 199–203.

[58] D. J. Bernstein, M. Hamburg, A. Krasnova, and T. Lange, "Elligator: elliptic-curve points indistinguishable from uniform random strings," in *Proceedings of the 2013 ACM SIGSAC conference on computer communications security*, ser. CCS '13. New York, NY, USA: ACM, 2013, pp. 967–980.

[59] "ETSI EN 319 411-1. Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements," European Telecommunications Standards Institute, Tech. Rep., August 2017.

APPENDIX

IFAL signature correctness. Here we show that the signature tuple (r, s') output by the `MessageSign` algorithm is a valid signature with respect to pseudonym public key P_i generated by the `GenCertFile` algorithm. Where $k \xleftarrow{\$} \mathbb{Z}_n \setminus \{0\}$ is the ephemeral key generated by the `Sign` algorithm and $k_{\text{cert}} = \mathcal{K}_1(k_{\text{epoch}}, i)$ is the key derived from an activation code by the `MessageSign` algorithm

$$
\begin{aligned}
r &= x \; mod \; n \\
s &= k^{-1}(h' + k_{\text{TE}} * r) \; mod \; n \\
\therefore s &= k^{-1}(h * k_{\text{cert}}^{-1} + k_{\text{TE}} * r) \; mod \; n \\
s' &= s * k_{\text{cert}} \; mod \; n \\
\therefore s' &= k_{\text{cert}} * k^{-1}(h * k_{\text{cert}}^{-1} + k_{\text{TE}} * r) \; mod \; n \\
\therefore s' &= k^{-1}(h + k_{\text{cert}} * k_{\text{TE}} * r) \; mod \; n \\
P_i &= \mathcal{K}_1(k_j, i) \times P_{\text{TE}} = k_{\text{cert}} * k_{\text{TE}} \times G
\end{aligned}
$$

Hence, (r, s') is a standard ECDSA signature with respect to the private key $k_{\text{cert}} * k_{\text{TE}}$. □