Footprint Analysis for IntelliDrive[SM] V2V Applications, Intersection Safety Applications, and Tolled Facilities

Pre-Decisional Discussion Document

March 2009

Prepared for the Intelligent Transportation Systems Joint
Program Office, Research and Innovative Technology Administration

Contract #: DTFH61-05-D-00002

noblis
For the best of reasons

Table of Contents

1. Overview

The IntelliDrive[SM] program is a joint public/private program[1] for enhancing safety and providing traffic management and traveler information. It uses "advanced wireless communications, on-board computer processing, advanced vehicle-sensors, GPS navigation, smart infrastructure, and others—to provide the capability for vehicles to identify threats and hazards on the roadway and communicate this information over wireless networks to give drivers alerts and warnings"[2].

In order to provide the low latency, high availability data communications required for safety applications, a technology called Dedicated Short Range Communications (DSRC), operating in the dedicated 5.9 GHz band has been developed. DSRC provides high bandwidth, low latency mobile data communications over short range (on the order of hundreds of meters). Other applications with less stringent requirements might also communicate using DSRC, or they could use alternatives such as 3G cellular or mobile WiMax.

The equipment on board a vehicle, including the DSRC radio, is typically referred to as On-Board Equipment (OBE). DSRC radios located along the roadside are part of what is referred to as Road Side Equipment (RSE).

1.1 IntelliDrive Applications

Many safety-related applications are possible using the sensing and high-speed communication capabilities provided by IntelliDrive. Vehicle-to-vehicle (V2V) applications between OBEs could enable a vehicle that brakes suddenly to warn nearby vehicles, enabling safer braking for them. Warnings of hazardous conditions detected by a vehicle (e.g., slippery conditions identified by the engagement of traction control systems) could similarly be communicated to nearby vehicles.

Other IntelliDrive applications involve vehicle-to-infrastructure (V2I) and infrastructure-to-vehicle (I2V) communication. These include systems where infrastructure RSEs broadcast safety-related warnings to approaching vehicles. The infrastructure may collect environmental and situational data from other vehicles or from land-based sensors such as cameras or weather sensors. Examples of warnings include bridge out, slippery road surface, or hidden traffic approaching an intersection. V2I and I2V communications can also support collection of vehicle speed and congestion information and provision of traveler information services back to drivers.

---

[1] A coalition has been established to support IntelliDrive research and determine the feasibility of widespread deployment. The coalition consists of the U.S. Department of Transportation, light vehicle manufacturers, state and local governments, and their representative associations. For more on the coalition, see http://www.intellidriveusa.org/coalition/.

[2] http://www.its.dot.gov/intellidrive/intellidrive_overview.htm

V2V traffic safety data mentioned above can also be relayed back to local Department of Transportation (DOT) facilities for further diagnosis of traffic congestion and physical infrastructure conditions. For example, multiple instances of traction control engagement warnings in the same geographic region may indicate the need for road treatment chemicals in inclement weather or road repair in general. Another stated purpose of the original VII system is to use GPS data from OBE-equipped vehicles to help DOT enhance existing maps with individual lane accuracy and to add new roads automatically as they are being built.

A third type of application is vehicle-to-device (V2D), where warnings may be transmitted to various devices such as cell phones or traffic control devices.

1.2 Purpose of this White Paper

The deployment approach and business model for rolling out IntelliDrive have not yet been decided. Several candidate approaches for initial deployment have been discussed by various stakeholders, including:

- Beginning with V2V safety applications and subsequent expansion to include intersection safety applications, and

- An approach that begins with deployment on priced roadways, including toll roads and High Occupancy or Toll (HOT) lanes.

This White Paper presents "order of magnitude" estimates of the number of roadside DSRC locations that would be required for three different sets of applications:

- To support only V2V safety applications
- To support V2I intersection safety applications
- To equip toll roads and HOT lanes

The number of roadside DSRC locations (RSEs) required in each case is referred to as the DSRC footprint requirement. The footprint requirements for these three cases are subsets of the footprint requirement for more extensive IntelliDrive deployments where the infrastructure collects safety, weather, and situational data from vehicles, processes it, and redistributes it to vehicles. Such applications may take advantage of whatever RSEs are installed for the initial deployments described in this White Paper.

As will be discussed in Section 3, the footprint required for supporting V2V safety applications is driven by the need for secure and private communications supported by infrastructure-based systems. The security and privacy requirements for IntelliDrive, as they are currently defined, are summarized in the next section. Two options are examined: one providing *anonymity by design*, and one providing *anonymity by policy*. These two concepts are defined in Section 2.2.

2. Security and Privacy

2.1 Security Model

Data security and authorization are essential components for most IntelliDrive applications. The effectiveness and safety of the applications could be significantly compromised if erroneous information is transmitted, received, and processed. The erroneous information could come from someone with malicious intent, by someone trying to "beat the system" or by malfunctioning equipment.

The most widely accepted standard for scalable secure communication is Public Key Infrastructure (PKI). Conventional PKI provides confirmation to the receiver of a message that the message sender is who he or she claims to be, and that the message did not suffer corruption during transmission (referred to as source authentication and message integrity). Encryption, decryption, and authentication are accomplished using a pair of complementary cryptographic "keys", one public and one private.

With PKI, messages are accompanied by digital certificates, issued by a trusted Certification Authority (CA). Digital certificates typically bind a public key to an identity, as vouched for by a trusted CA, much like a state issued driver's license binds the holder's facial picture and signature to his or her printed name and postal address. IntelliDrive also adds *anonymous* digital certificates, which are computationally equivalent to standard PKI digital certificates, but do not contain the certificate holder's name or identifier. In this case, an anonymous digital certificate still provides data integrity, but is to be interpreted as an indicator of authorization to transmit (much like driver's licenses are also indicators of authorization to operate a motor vehicle). Appendix A provides a brief overview of PKI and how it has been adapted for use in IntelliDrive applications.

2.2 Privacy Model

From the beginning of IntelliDrive, privacy has been a major concern. Most people are not comfortable with the idea of a computerized system that has the capability of tracking the location of individual vehicles for extended periods, and, by extension, tracking the location of individual persons. Nor are people comfortable with the perception that their presence and movement in a geographical area could be broadcasted to others. The public is all too familiar with news of governmental and corporate data systems that were supposed to protect the private information they contained, but from which personal data was stolen by insiders or outsiders, sometimes with very negative results.

The planners of IntelliDrive applications are keenly aware of the public's wariness of the potential for abuse that is present when personal driving data is stored. Even the collection of the data without storing it is a potential problem for many people. The major auto manufacturers have clearly stated they are aware of the public's strongly held belief in rights to privacy and have observed behavioral evidence that the public will not participate in IntelliDrive if the public feels their privacy will be violated. The VII[3]

[3] Vehicle Infrastructure Integration, former name of the IntelliDrive program

Coalition approved a consensus document outlining the project's guiding principles on privacy.[4] Moving toward implementing these principles, the IntelliDrive planners have articulated the policy called "Anonymity by Design." According to this policy, opportunities for collecting or combining data in such a way as to reveal the travel behavior of any individual or vehicle are significantly minimized. To the greatest extent possible, data is collected and processed anonymously. That is, information that could be used to identify a particular vehicle or trace a vehicle over any but the shortest of distances[5] is not technically correlatable.

The terms "anonymity by design" and "anonymity by policy" have been frequently used in IntelliDrive privacy discussions, but they have not been formally defined. In this paper, we propose the following definitions. "Anonymity by design" means that multiple technical controls have been built into the system to ensure that, to the maximum extent possible, a vehicle's or person's identity can not be determined based on their IntelliDrive data exchanges, or based on what was captured in one system's log file. This constraint would not apply to systems that by their very nature require individuals to opt-in voluntarily and identify themselves, such as toll payment applications.

Under the current envisioned implementation, one would have to tap into a real-time data stream and have access to logs from two separate protected certificate authorities in order to track an individual vehicle or obtain the sender's identity. A system that could enable vehicle tracking or identity discovery with access to fewer than two separate protected authorities would not qualify as providing anonymity by design under this definition. This paper assumes that this level of anonymity by design is a program requirement. It is beyond the scope of this paper to discuss the pros and cons, or the implications of this approach. Details and implications of the "Anonymity by Design" policy are discussed in a Noblis White Paper *Anonymity and IntelliDrive*[SM] .[6]

"Anonymity by policy" means that a user's privacy is protected through adherence to written policies. If one person employed in the right place within an IntelliDrive system violated the policy, private data could be divulged. However, for IntelliDrive, many privacy protection mechanisms would still be included in the architecture. For example, personally traceable information would be stripped off at the earliest opportunity in the data flow, and any information not needed for the specific purposes of IntelliDrive applications would not be retained. Policies, regulations, and possibly laws would be put in place to limit access to the data.

A typical PKI deployment does not inherently provide for anonymity. In fact, it is designed to provide for message authentication (proving exactly who sent the message) and message non-repudiation (the sender cannot deny sending the message). For

---

[4] Jacobson, L., February 16, 2007, *Vehicle Infrastructure Integration Privacy Policies Framework Version 1.0.2*, Institutional Issues Subcommittee, National VII Coalition.

[5] In a VIIC Security Working Group meeting, it was agreed that "trackability" would be defined as the ability to determine vehicle movement beyond what one stationary human could visually observe.

[6] Gonzalez, P. and M. McGurrin, February 2009, *Anonymity and IntelliDrive*[SM], Noblis.

IntelliDrive, the method of employing PKI has been augmented to provide anonymity for privately owned vehicles. Section A.2 of the Appendix describes the proposed method for using PKI while maintaining anonymity. There is no requirement for the identity of the sender to be established; rather the requirement is to determine that the sender is among the set of authorized users. Therefore, digital certificates in IntelliDrive are tokens of authorization to transmit. Users that are identified as "bad actors" have their authorization revoked via standard Certificate Revocation Lists (CRLs).

3. Footprint Required to Support V2V Safety Applications

If it were not for the security considerations presented in Section 2.1, V2V communications for safety applications would not need to have a V2I component. Warning messages could be transmitted directly and anonymously to any vehicles with OBEs that are within DSRC communication range. However, security considerations for guarding against malicious, manipulative, or corrupted messages require that messages be digitally signed and accompanied by valid certificates. Certificates can be requested and issued only through some periodic contact with the IntelliDrive infrastructure.

If OBEs participate in the identification of potential "bad actors" (see Appendix Section A.3) and upload that information to the infrastructure, the uploads are a form of safety-related V2I communications that may use DRSC. This analysis assumes that any RSE footprint required for certificate management would also satisfy any requirement for uploading potential bad actors.

IntelliDrive safety applications may also include I2V communications including:

- Downloading Certificate Revocation Lists (see Appendix Section A.3)
- Obtaining clock and GPS drift corrections
- Weather alerts.
-

These I2V communications could use DRSC, or they could use alternative communications methods, including general broadcasts, e.g., on a commercial FM radio subchannel.

The following subsections estimate the DSRC footprint for the cases where anonymity by design is implemented by DSRC or by cell phone and Wi-Fi technology.

3.1 Features of Anonymity by Design

The process of using PKI for communication requires all message senders to obtain one or more certificates from a Certification Authority (CA). The CA is responsible for verifying that the would-be sender is legitimate before a certificate is issued. A valid certificate must be part of every transmission. To make it more difficult to track a single vehicle by looking for matching certificates, senders will be issued multiple certificates from a large pool of valid certificates, and duplicate certificate numbers and corresponding cryptographic key pairs will be assigned to multiple OBEs. For the same reason, certificates will be changed periodically. In most PKI implementations, certificates are valid for months or years. However, in order to ensure that a long history

does not enable the tracking of individual OBEs, under this approach they will expire within days or weeks, and be replaced with new certificates and key pairs. The size of the pool, the number of certificates in a bundle, and the time interval at which certificates expire and must be replaced have not yet been determined. Appendix A discusses these features in more detail.

The process of how vehicles will request and receive a bundle of valid certificates is discussed in Appendix Section A2, Step 4. However, if anonymity is to be preserved, the communications options are limited.

3.2 Footprint Assuming Anonymity by Design and DSRC Communications

If DSRC is used as the communications technology, in order to preserve anonymity, a large footprint is required, since every vehicle must pass within range of an RSE to obtain new certificates before its current pool of certificates expires. Under the current thinking, this certificate refresh would need to occur somewhere between every few days and every few weeks, but the IntelliDrive community has not reached consensus on the refresh rate that would be required.

Most vehicles visit gas stations with this frequency already, so gas stations might be a logical location for these RSEs. There are approximately 130,000 gas stations in the United States[7], so that is an upper bound on the number of RSEs required for this scenario. Most likely, there would not need to be an RSE at every gas station. For example at intersections or strip malls where there are multiple gas stations in close proximity, only one need be so equipped. Deploying RSEs at one-quarter to one-half of the nation's gas stations would require 32,000 to 65,000 RSEs.

An additional advantage of placing RSEs at gas stations is that vehicles remain stationary there for at least several minutes. This simplifies communications since the entire transaction can be completed while the OBE is in communication within the range of one RSE.

An alternative approach would position RSE's along the roadside, especially at signalized intersections and freeway interchanges. Previous analysis[8] has determined that approximately 100,000 locations would be required to equip 20% of the signalized intersections in the U.S., interchanges and intersections along the National Highway System[9], and other locations where there would otherwise be long stretches without communications.

---

[7] http://www.census.gov/econ/census02/data/industry/E447110.HTM

[8] Mitretek Systems, 19 December 2005, *VII Road Side Equipment (RSE) Deployment Analysis: Results of Sensitivity Analyses*.

[9] The National Highway System consists of 160,000 miles of roadway. It includes the Interstate Highway System as well as other roads important to the nation's economy, defense, and mobility. See http://www.fhwa.dot.gov/planning/nhs/ for additional information.

3.3 Footprint Assuming Anonymity by Design and Cell Phone or WiFi Communications

The estimates of RSEs in the previous section assume that RSEs need to be situated in places for convenient anonymous access by vehicles. It may be possible to design an architecture to request and receive anonymous certificates using cell phone or WiFi technology while still satisfying the requirements of anonymity by design. In this case, the requirement for a separate infrastructure to support V2V applications can be eliminated.

A 2008 study indicated that 84% of the U.S. population own cell phones, for a total of 262 million subscribers.[10] Almost half of these subscribers are already using some form of wireless data.[11] Either the OBE could itself have a cellular data link or utilize a wired or wireless (e.g., BlueTooth or Wi-Fi) link to communicate data using a cell phone. This cell phone base could go a long way toward IntelliDrive deployment, provided it can be both secure and anonymous.

In order to meet the definition of "anonymity by design" for certificate management, the over-the-air link must be adequately encrypted (in addition to the end-to-end encryption between the OBE and the certificate authorities). This wireless link encryption is needed so that an eavesdropper cannot determine the source and destination IP addresses for the message, and then match the time of the message with a transaction record in the identify certificate authority. The cell tower will be able to decrypt only the IP address of the Anonymous CA to which a certificate request is addressed, so it can forward the message.

Current GSM (Global System for Mobile communications) encryption may not be strong enough for this purpose, but third generation (3G) and future cellular technology is expected to be more secure *provided it is implemented on a consistent basis by all carriers throughout the U.S.*

However, it is important to note that cell phone communication cannot be anonymous as far as the service provider is concerned. Each cell service provider knows the identity of each unit it supports and can track its location. The end-to-end encryption of message payloads ensures that the cell phone provider or one of its employees cannot determine anything about the certificates that are provided. However, if cell phones were to be mandated for IntelliDrive applications that require frequent messages such as probe

---

[10] International Association for the Wireless Telecommunications Industry, http://www.ctia.org/advocacy/research/index.cfm/AID/10323

[11] International Association for the Wireless Telecommunications Industry, http://www.ctia.org/advocacy/research/index.cfm/AID/10383

messages, the anonymity by design concept would be violated, since the cellular provider could keep a record of each subscriber's travels.[12]

Millions of Americans also have wireless Internet connections using Wi-Fi technology based on IEEE 802.11 standards, and public Wi-Fi hotspots exist throughout the country. Provided that strong over-the-air encryption such as EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) as called for in the Wi-Fi Protected Access 2 (WPA2) certification program is used, this would provide another option with anonymity levels similar to that provided by the cell network. To ensure against "man-in-the-middle" attacks, the OBE should verify the security certificate of the Wi-Fi access point. An OBE would need to be equipped for Wi-Fi communications with the access point in order to use this approach.

If the anticipated over-the-air security is not considered adequate, an additional element could be added to the IntelliDrive architecture to provide the desired level of anonymity. A small number of anonymizing portals could be established through which all IntelliDrive communications would pass. OBE requests for certificates via cell phone would encrypt the payload for the IntelliDrive portal and would be transmitted via secure HTTP (HTTPS). The IntelliDrive portal would function like a stateful source Network Address Translating firewall, meaning that the source address changes as it enters the IntelliDrive network, but the portal firewall knows how to deliver return data. A more detailed description of this communication is presented in Appendix B.

An eavesdropper might be able to see the source/destination IP addresses, but this would only be the address of the IntelliDrive portal, and therefore the nature of the payload or its ultimate destination could not be derived. So, even if the eavesdropper could find one colluding individual at the Anonymous CA, it would be very improbable that they would know what timestamp to look for in the Anonymous CA logs since the OBE makes so many transmissions through the IntelliDrive portal. This architecture would satisfy the requirement of anonymity by design.

4. Footprint Required to Support Intersection Safety Applications

Another model for deployment of RSEs would place them at major signalized intersections. This would be done to reduce crashes by enabling Cooperative Intersection Collision Avoidance Systems (CICAS)[13].

Crashes are not uniformly distributed across intersections. A study of three major U.S. cities (Detroit, San Francisco, and Orlando) revealed that when intersection are ranked in descending order of the number of collisions, approximately 50% of intersection collisions occur at intersections in the top 20% of the list, and 80% of such collisions

---

[12] Cellular providers can do this today, however, use of the cellular system is not mandatory. This issue is discussed further in section 6.

[13] http://www.its.dot.gov/cicas/index.htm

occur at intersections in the top 50% of the list. The results were remarkably similar for the three cities studied.[14]

There are approximately 260,000 signalized intersections in the United States. Assuming that nationwide collision statistics are similar to those in the three cities examined, the table below indicates the number of RSEs required nationwide to provide certificates and to prevent intersection collisions in a CICAS application at these two percentage levels.

Percentage	Percent of Collisions Avoided	Number of RSEs Required
20%	50%	52,000
50%	80%	130,000

5. Footprint Required for Toll Roads and HOT Lanes

One option for initial "tactical" deployment of RSEs is to combine electronic toll collection with other IntelliDrive services. Initial deployment would occur along toll roads and HOT lanes. These facilities are logical choices for early deployment because electronic toll collection equipment is already installed, and vehicle drivers using those facilities have already opted in to electronic communication. The safety and traffic information benefits of participation in IntelliDrive could be promoted as additional benefits of paying the toll to travel on the "premium road".

For non-safety applications, this deployment could involve an aftermarket or brought-in device, rather than an OBE provided by the automaker.

According to the International Bridge, Tunnel, and Turnpike Association, in 2007 there were over 15 million toll tag accounts in the United States, and over 26 million toll tag transponders[15].

As of 2007, there were approximately 2,694 centerline miles of urban toll road facilities in the United States, 2,223 centerline miles of rural toll roads, and 114 centerline miles of HOT lanes[16]. The number of RSEs required to cover these toll roads was computed by using the previous Noblis study, which estimated that RSEs would be required every four centerline miles along an urban road, and every twenty centerline miles along a rural road.[17]

Applying the RSE spacing listed above yields the following numbers of RSEs.

Type	Number of Miles	RSE Spacing	Number of RSEs

[14] McGurrin, M. and J. Bunch, *RSU Deployment Analysis*, VII Working Group Meeting, 5 May 2005.

[15] 15,728,283 accounts and 26,647,687 tags, from *Toll Facility Tags and Accounts*, 2007, International Bridge, Toll, and Turnpike Association.

[16] Publication No. FHWA-PL-07-029

[17] Op. cit., McGurrin and Bunch.

Urban toll roads	2,694	4 miles	675
Rural toll roads	2,223	20 miles	112
HOT lanes	114	4 miles	30
Total	5,031		817

The "bottom line" is that all existing toll roads and HOT facilities could be fully instrumented with less than 850 RSEs.

6. Deployment Issues

Participation in the IntelliDrive program may be mandatory or may be optional. In the former case, all new vehicles will be required to feature operational OBEs. Universal participation would be required because of the public good that would result, including safety and traffic management. In the latter case, drivers may choose to buy new vehicles with an OBE or to install an after-market OBE and to participate in the program on the basis of personal or societal advantage. The latter arrangement is sometime called "opt-in." Examples of current opt-in systems are OnStar and all toll tag systems.

On another axis, IntelliDrive systems may be implemented either with or without "Anonymity by Design." In the latter case, privacy would remain an important principle, with personally identifiable information stripped off at the earliest opportunity. Implementation of the system without anonymity by design is much simpler, since neither an RSE footprint nor anonymizing portals would be required. The drawback, of course, is that anonymity is not guaranteed as strongly.

Conceptually any box in the following diagram could represent the status of IntelliDrive applications as they come to wide-spread existence. The IntelliDrive community must determine which box will most closely define the applications. It is possible that the community will decree that the bottom left box, representing mandatory participation but anonymity by policy, will not be considered as an option. On the other hand, anonymity by design may be judged too complex and expensive.

	Participation Requirement	
Anonymity Protection	Mandatory participation Anonymity by design	Opt-out allowed Anonymity by design
	Mandatory participation Anonymity by policy	Opt-out allowed Anonymity by policy

7. Summary

If the anonymity by design using only DSRC communications is followed, even V2V safety applications will require a large DSRC footprint, on the order of 30,000 to 130,000 locations.

For purposes of certificate management, an approach using cellular communications and/or Wi-Fi could be implemented in a manner that meets the anonymity by design definition. However, this is only true if adequate over-the-air security is in use by all cellular carriers throughout the U.S. and/or by all Wi-Fi locations used by IntelliDrive. In addition, use of this media for more general IntelliDrive applications would violate the anonymity by design concept.

Equipping 20-50% of intersections in order to support CICAS, would locate these devices at locations where 50-80% of intersection crashes occur, and would require 52,000 to 130,000 locations.

The existing network of toll roads and HOT lanes would require less than 850 locations. While this provides only a minimal infrastructure footprint, the 15 million electronic toll accounts in the U.S. offers a large pool of potential users.

8. Caveats

The above analysis and summary should be weighed against other important operational details yet to be considered:

- Choosing an alternative to DSRC communications for applications such as probe data, certificate management, payments, etc., does not remove the need for DSRC communications in the vehicles. That is, choosing an alternative to DSRC really means that the vehicles will now need to be equipped with two communications technologies. However, choosing an alternative to DSRC does mean that deployment of a large DSRC footprint will not be necessary.

- DSRC is still the best candidate for high-bandwidth, low-latency applications, such as V2V safety applications.

- Depending on the enforcement requirements of IntelliDrive automatic tolling, (which may or may not differ from EZ-Pass automatic tolling), payment data exchanges at highway speeds may also require high-bandwidth, low-latency communications. This would require DSRC footprint deployment along HOT corridors.

- Further studies are needed to determine if commercial cellular services can handle the increased load consisting of IntelliDrive communications.

- A proof-of-concept system is needed to demonstrate how the anonymous cryptographic key pairs can be stored in such a way that they cannot be stolen or copied.

- While the 2008 study mentioned above shows that a significant percentage of the public subscribes to a cellular service, often cell phones cannot transmit data while already engaged in voice communication and fewer citizens subscribe to data plans.

Appendix A Basics of PKI

A.1 Authentication Using PKI

Typically, a public key infrastructure works as follows. The frequency of the first two steps may vary. Steps 3 through 6 are executed for each message sent.

1. The sender either (a) produces its own public/private cryptographic key pair and applies for a digital certificate from a trusted Certification Authority (CA), or (b) requests the CA to generate the public/private key pair for the requestor and to provide the associated digital certificate. Typically a certificate is valid for several years, but for anonymous IntelliDrive applications the certificates may need to be renewed much more frequently.

2. Upon satisfactory proof of identity, the CA generates the public/private key pair if requested, and in either case the CA issues and signs the digital certificate with its own digital signature. As mentioned above, the frequency of certificate issue for IntelliDrive applications has not yet been finalized, but is expected to range from days to weeks if anonymity by design is required.

3. The sender digitally signs the message and sends it, together with the certificate.

4. The receiver performs a data integrity check and verifies the digital signature using the sender's public key contained in the certificate.

5. The receiver verifies that the certificate is valid by (a) using the public key of the issuing CA found in a locally stored copy of the CA certificate and (b) checking the current certificate revocation list.

6. If the certificate is not valid, the message is discarded.

A.2 Providing Anonymity for IntelliDrive Using PKI

Typically the PKI scheme outlined above provides authentication and non-repudiation (establishes the identity of the sender) and guarantees the integrity of the message through transmission. However with anonymity by design, it is important that the identity of the sender can not be established, only the fact that the sender is authorized to send with a legitimate and valid certificate.

Therefore, the current IntelliDrive plan for approving and issuing anonymous certificates for IntelliDrive applications has the following four main features[18]:

1. Rather than being issued a single public/private key pair in a certificate, the vehicle will be issued a bundle of certificates with the corresponding public/private key pairs. These certificates are stored in the OBE. Whenever the OBE transmits a message, it chooses randomly from its collection of valid certificates. The more certificates there are in a bundle, the less likely that someone could correlate a set of transmissions from a single vehicle. The number of certificates in a bundle has yet to be determined.

2. Multiple vehicles will be issued the same anonymous certificates and key pairs. The use of the same certificates by multiple vehicles is a further deterrent to the ability of anyone to correlate the transmissions from a single vehicle. Since the certificates are used to establish authority to send rather than to establish sender identity, the duplication of certificate numbers and key pairs is permissible (although it complicates bad actor detection and certificate revocation, as discussed in section A.3).

3. The anonymous certificates in a vehicle's bundle will expire periodically. The resulting change of anonymous certificates is a further deterrent to the ability of anyone to correlate the transmissions from a single vehicle. The length of time for which certificates are valid and whether they will all expire at the same time or have staggered expiration times have not been determined.

4. The following procedure has been devised so that no single agency could have records linking a given anonymous certificate to a given vehicle. The job of the Certification Authority (CA) will be split among two entities: an "anonymous CA" and an "Identity CA". The former issues the anonymous certificates and the latter verifies the identity of the requester to ensure the requester is authorized to obtain certificates. This occurs as follows:

    a. When a vehicle needs to renew its certificates, it sends a request to the Anonymous CA. A portion of the request is encrypted to be read by the Identity CA, but the request also contains an unencrypted temporary ID by which it is identified to the anonymous CA. The request is sent from the vehicle to the Anonymous CA, and the Anonymous CA forwards the encrypted portion to the Identity CA.

    b. The Identity CA receives the request and decrypts it. It checks the validity of the requester, including checks that:

[18] These features are part of the current IntelliDrive approach. They may be re-examined as part of the planned architecture revision work. For the purposes of this paper, they were taken as requirements that had to be met.

i. The requesting vehicle has a valid Vehicle Identification Number (VIN)
ii. The vehicle is not on the "bad actor" list
iii. The vehicle has not requested an inappropriately high number of certificates recently

c. The Identity CA notifies the Anonymous CA whether or not the request has been approved.

d. If the request is been approved, the Anonymous CA generates or retrieves from its local store a bundle of anonymous certificates and corresponding key pairs and transmits them to the requesting OBE.

Because of the way that the duties for issuing certificates are split between the two CAs:

- The Identity CA knows what OBE has requested certificates, but not which certificates have been issued.
- The Anonymous CA knows which certificates have been assigned and transmitted to the OBE, but not the identity of that OBE.

In this way, the identity of an individual or vehicle can be determined only through a court order or other legal procedure decreeing that the records from the two CAs must be combined to yield the identity of the OBE to which a specific anonymous certificate was issued. The fact that the same anonymous certificate may be issued to multiple OBEs makes the correlation more difficult, even if it is court-ordered.

A.3 Bad Actors and Certificate Revocation Lists

A "Bad actor" is an OBE determined to be unreliable or malicious, and therefore should not be permitted to send IntelliDrive messages. Possible types of bad actors are:

- Terrorists
- Criminals
- Hackers
- Persons trying to "game" the system
- Malfunctioning equipment

Bad actors may be determined when messages are found to be repeatedly incorrect, or when a single OBE requests anonymous certificates too frequently, or there is other suspicious activity. An identified bad actor:

- Will be refused when it applies for new certificates
- Will have its existing certificates revoked. The certificates will be placed on the Certificate Revocation List (CRL) which is updated frequently and disseminated throughout the system.

There are at least four issues associated with CRLs:

- When a certificate is placed on the CRL because it has been revoked, all other legitimate OBEs that have been assigned the same certificate can no longer use it. We refer to these OBEs as “innocent victims.” They will have to use alternate anonymous certificates until it is time for them to get a new bundle of certificates.

- A bad actor can continue to use the system until all of the certificates in his or her bundle have been revoked or a yet-to-be-determined low threshold number of certificates remain. In addition, if only some of the certificates have been revoked, a bad actor could use a still valid certificate to request an entirely new batch of certificates.

- The method of disseminating CRLs has not been determined. CRLs may be transmitted by RSEs or by OBEs. However, a message containing a CRL must be verified that it comes from a valid user, just like any other IntelliDrive message.

- It has not been determined whether OBEs will participate in the process of identifying bad actors or whether that is strictly a function of the infrastructure.

Appendix B. OBE Communication With an Anonymizing IntelliDrive Portal

Section 3.3 presents the concept of a small number of portals through which all IntelliDrive communications would be routed, and which would safeguard the message IP addresses. This concept was developed during the course of this analysis, and is not currently part of the IntelliDrive security and privacy approach. This type of system could work as follows:

- The OBE encrypts an anonymous certificate request payload for the Anonymous CA.

- The OBE adds a wrapper to the payload, including a "type" byte indicating the nature of the payload (i.e., that it is an anonymous certificate request).

- The OBE does a standard Hypertext Transfer Protocol Secure (HTTPS) "PUT" to the IntelliDrive portal, passing along the "type" byte and the encrypted payload. The "S" in HTTPS prohibits eavesdropping of the contents of this exchange with the OBE. Only the source and destination IP addresses are observable.

- The IntelliDrive portal forwards the encrypted payload to the Anonymous CA (without the requestor’s source IP address).

- When the Anonymous CA responds with the anonymous certificate bundle (or the reject message), the IntelliDrive portal sends the response, still inside the HTTPS encrypted tunnel, to the OBE.

An eavesdropper might be able to see the source/destination IP addresses, but this would only be the address of the IntelliDrive portal, and therefore the nature of the payload or its ultimate destination could not be derived.

List of Acronyms

CA	Certification Authority
CICAS	Cooperative Intersection Collision Avoidance System
CRL	Certificate Revocation List
DOT	Department of Transportation
DSRC	Dedicated Short Range Communications
EAP-TLS	Extensible Authentication Protocol Transport Layer Security
IP	Internet Protocol
GHz	Gigaherz
GPS	Global Positioning System
GSM	Global System for Mobile Networking
HOT	High Occupancy / Toll
HTTPS	Hypertext Transfer Protocol - Secure
I2V	Infrastructure-to-Vehicle
OBE	On-Board Equipment
PKI	Public Key Infrastructure
RSE	Roadside Equipment
VII	Vehicle Infrastructure Integration
VIIC	Vehicle Infrastructure Integration Consortium
V2D	Vehicle-to-Device
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
WPA2	Wi-Fi Protected Access 2