Chapter 10
Security and Privacy for ITS and C-ITS

Scott W. Cadzow

Abstract Intelligent Transport Systems (ITS), and the specialised subset of them represented by Cooperative ITS (C-ITS), are part of the wider machine-to-machine communications, and software driven world. The aims of ITS and C-ITS are multifold but for the purposes of this book are mainly in improving safety of transport users and their transport modes. The chapter that follows covers some of the basics of security, including the contrast with safety and privacy, the role of privacy protection in the ITS context, and a review of the cryptographic countermeasures recommended for C-ITS using the certificate and signature schemes defined in IEEE 1609.2.

Keywords VANET • Security • Privacy • 1609.2 • Pseudonym • Integrity • Trust • Authenticity • Authority • Confidentiality • Pseudonymity • Algorithms • Cryptography • Certification • Verification • Validation • Cryptanalysis • Attack models • Defence strategy • ETSI • Standardisation

Acronyms

CA	Certification Authority
CIA	Confidentiality Integrity Availability
ECC	Elliptical Curve Cryptography
GSM	Global System Mobile (mostly deprecated)
IMEI	International Mobile Equipment Identifier
IMSI	International Mobile Subscriber Identifier
PIN	Personal Identification Number
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
SIM	Subscriber Identity Module

S.W. Cadzow (✉)
Cadzow Communications Consulting Ltd, Sawbridgeworth, UK
e-mail: scott@cadzow.com

C. Campolo et al. (eds.), *Vehicular ad hoc Networks*,
DOI 10.1007/978-3-319-15497-8_10

TEI	TETRA Equipment Identifier
TETRA	Terrestrial Trunked Radio (largely deprecated in favour of TETRA)
VIN	Vehicle Identification Number

10.1 Introduction

Intelligent Transport Systems (ITS) are a specialised subset of machine-to-machine communications in a software driven and all-connected world. There are a number of dimensions of ITS and different authors may present different lists of them but for the purposes of examining the security issues this list will suffice:

- Advanced Traveller Information Systems (ATIS),
- Advanced Traffic Management Systems (ATMS),
- ITS-Enabled Transportation Pricing Systems,
- Advanced Public Transportation Systems (APTS),
- Vehicle-to-Infrastructure Integration (VII), and,
- Vehicle-to-Vehicle Integration (V2V)

C-ITS sits in this list as a special case of both VII and V2V, with the functionality of C-ITS centred on the exchange of data between co-operating ITS stations.

The root concept behind C-ITS is that of giving machines some degree of spatial awareness, and using that spatial awareness to protect both their own space and the space of all other transport users. If we consider the thing that seems to concern most motorists more than anything else, it is fear of having a collision. This ranges from a little bump in a car park all the way to the catastrophic collision on a motorway. The basic idea of spatial awareness as a defence comes from martial arts—if you know where your opponent is aiming then make sure you're not there when his blow lands. Same in a car—if something is on a path to hit you make sure you're not there when the blow lands or be in a position where the damage is negligible.

Spatial awareness for a driver means being aware of where you and your vehicle are with respect to all other vehicles and the infrastructure in order to ensure that you are not encroaching on the safe zone around any other road user. In a conventional vehicle this means using your senses of sight and hearing to continuously build up a mental three-dimensional map of the other road-users around you and working to ensure you are "safe" with respect to them. This is done through constantly using mirrors, moving around to eliminate blind spots (not moving the vehicle but your body), listening for other vehicles and so forth. However in many ways the design of road vehicles has increasingly limited the ability of a driver to build up this 3-D mental map by being quieter, having more restricted visibility and having a number of distraction technologies to hand (e.g. phones, music, navigation tools). The excuse of "I didn't see you" is the first thing to be reported from far too many accidents and one of the roles of C-ITS is to eliminate the blind spot and allow vehicles to see each other in all environments.

One of the other concerns raised when C-ITS was first conceived is that by transmitting information that allows receivers to build up a spatial model of how your vehicle is interacting with it, the same data could be used to track you. C-ITS has been designed to operate in areas of the world where expectations of privacy are high and therefore the protection of users from being tracked, or of their transmissions being used against them, has been very high on the agenda and C-ITS has been built to maximise privacy protection.

The bulk of ITS types (ATIS, ATMS, APTS, etc.) are data centric, in that they gather and distribute data. What differentiates them is where the data comes from and who its intended recipients are. For VII and V2V, and more specifically C-ITS, data comes from the co-operating vehicles and is intended for those vehicles. In the native environment in which vehicles find themselves the safety of any individual vehicle is determined by a set of factors that include:

- Driver awareness,
- Vehicle road-worthiness,
- Road conditions,
- Weather conditions,
- Traffic signalling,
- Relative velocity,
- Other vehicles

What C-ITS will achieve, at least in intent, is greater driver awareness by giving authoritative information to the driver on their relative velocity and the presence of other vehicles and their vectors. The key term is "authoritative information". The purpose in C-ITS security is to assure the receivers of C-ITS data that it genuinely comes from a vehicle and is an accurate representation of the location and nature of the vehicle. The remainder of this chapter considers how security techniques applied to C-ITS give that assurance. In Sect. 10.2 we first examine the meaning of security expanding this in Sect. 10.3 looking in more detail at trust, and in Sect. 10.4 at privacy. In Sect. 10.5 the topic of identity is examined with Sect. 10.6 looking at symmetric and asymmetric security. Section 10.7 reviews the standards supporting C-ITS security and in Sect. 10.8 some conclusions are drawn.

10.2 Security

First we need to be clear by what we mean by the term security as it is easily confused with safety and with privacy. In order to assist in clarifying this we will quickly look at each of safety and security, privacy (defined as a state in which one is not observed or disturbed by other people) will be dealt with in more detail later.

When looking at the use of transport on the public highway safety is the dominant concern of most users, where safety is defined as the condition of being protected from, or unlikely to cause, danger, risk, or injury. Safety is improved in many ways and the result is essentially less likelihood of danger, risk or injury. In addressing

Fig. 10.1 US DoT mockup of how C-ITS may give awareness

safety improvements we can consider a number of areas that improve fundamental safety and this has, over time, included better road surfaces, better tyres, improved braking and dynamic performance of vehicles, which together allow an aware driver to be able to drive around a risk (e.g. by being able to brake without skidding, or being able to brake and turn at the same time without terminal understeer or oversteer). In addition there is much done to protect the passengers of vehicles when they do crash by designing in crumple zones (allowing the car to deform in a controlled way to absorb impact), improving driver and passenger restraint systems (both seat belts and airbags which prevent the driver or passenger becoming an uncontrolled projectile in the event of an impact), and there have been improvements in road design and lighting to minimise the likelihood of accidents due to the local geography (e.g. identifying and removing adverse camber on corners, improving street lighting at dangerous junctions). Figure 10.1 aims to illustrate how C-ITS can give awareness through all-informed "here I am" transmissions.

It could be argued that greater segregation of drivers will be the next stage in improving safety but giving every vehicle complete segregation from every other is simply not practical. So we are looking at extending the core requirement of driver's being aware of the road and vehicles around them to the vehicles sharing contextual knowledge with each other to give the possibility of virtual segregation (i.e. vehicles declaring a protected geographic zone around them).

In contrast with safety, security (and security technology) is considered as safety enhancing. The paradigm in conventional security is CIA—Confidentiality, Integrity, Availability—and so in the domain of ITS Security we are looking at means of using security technologies to augment safety technologies. Furthermore within the C-ITS Security domain we are seeking means of preventing abuse of the wider technology that may lead to reduction in safety (more risk).

The starting point for the development of ITS security has taken the following as targets:

- Messages must be secure
  - Broadcast messages cannot be spoofed
  - Unicast messages cannot be spoofed or eavesdropped

- Anonymity for end-user vehicles and their occupants
  - Messages (either individually or as sets) do not give away (reveal) identity
- Must be able to remove bad actors

As secondary characteristics for the development of ITS security solutions the following have also been considered:

- Overhead due to security must not be excessive
  - 200 bytes probably okay, 1,000 bytes probably not
- Vehicles may have to receive hundreds of messages per second and must be able to process them

In the security world the primary term to work against is risk, where the risk of something happening is a combination of the impact of it happening and the likelihood of it happening. Reducing the impact of two vehicles colliding is addressed through the design of the vehicles. This is where crumple zones, airbags, seatbelts, Anti-lock Braking Systems (ABS) and all other three-letter acronyms we see in the sales literature for cars play their part. Of course not all parties in collisions are in equally protected vehicles, some of the parties will be cyclists or pedestrians, in some cases the collisions will be with buildings or our road furniture (e.g. lighting systems, lane division bollards), in which case the approach to minimising risk is to minimise the likelihood of collision.

The relationship of security technology to risk is clear: Risk reduction and risk assurance can be managed by the targeted application of security measures (shown in Fig. 10.2) but only if you know about the risk in the first place.

In the development of ETSI's security standards and the services they invoke the means to perform a risk analysis followed the broad outline given in ETSI TS 102 165-1 [1] and whose process is illustrated in Fig. 10.3.

Fig. 10.2 The process of risk management and risk assurance

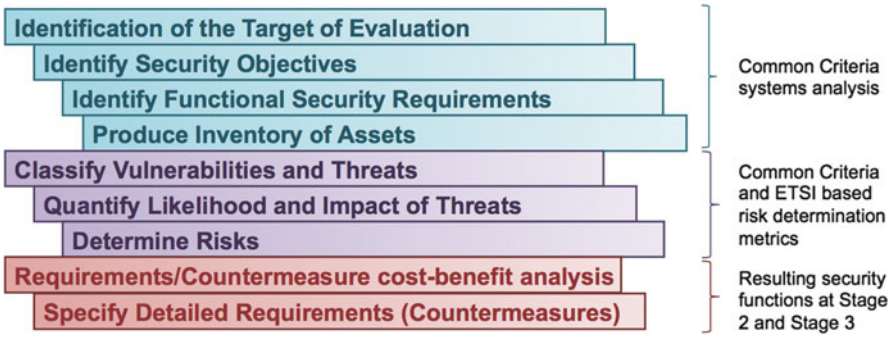

Fig. 10.3 The ETSI standards based Threat Vulnerability Risk Analysis (TVRA) process

In moving towards a safety system that is built on data transmitted from other vehicles we need to ask: Is the data complete? Is the data accurate? It is probably safe to say that the concept of C-ITS is built up by the continuous broadcast from every vehicle of a Cooperative Awareness Message (CAM), the content of which basically says "I am a vehicle of type x and I am at location y at time z". Additional information can be added to this but that is the essence. In addition there is a second form of message transmitted, a Decentralized Event Notification Message (DENM). The second message can take many forms but in essence says "I am reporting event x happened at location y at time z", where the event could be a weather event, a queueing event, an accident event or something else. So it may be that a car has detected ice and reports that. For a detailed discussion about CAMs and DENMs, see Chap. 5.

The way in which the receiver acts on this data determines to some extent the contribution to safety of C-ITS. In addition if a malicious actor can introduce false data to the system how would this impact the system. The problem with data is that it is somewhat intangible and how we react to it depends on two things: Context and Trust.

10.3 Context and Trust

When looking at context, particularly for C-ITS, we need to determine is the information offered of value to me? In other words, is the data relevant to my context?

Trust is rather more complex in that it means do I believe the data to be accurate and does it assist me in building a complete model of the environment? It also means do I trust the sender of the data?

Establishing trust is difficult and has a very human interpretation. Trust is also contextual and this will be examined in more detail later. It may be worth using analogy to examine trust: I trust Bob when playing tennis as my doubles partner

so in the context of a tennis court (on my side) I trust Bob's judgement and his instructions; Away from tennis Bob is a car mechanic and offers me financial advice. On what basis should I trust Bob in this new context? For this we mentally create trust relationships which we contextualise and which we modify over time. This leads to some commonly ignored attributes of trust:

- Trust is not a binary operation. There may be various levels of trust that an entity has for another.
- Trust may be relative, not absolute. Alice may trust Bob more than Eve, without trusting either absolutely.
- Trust is rarely symmetric and should never be made artificially so. Alice may trust Bob completely, whereas the amount of trust that Bob has for Alice may be very low. The pupil may trust the master without any requirement for that trust to be reciprocated.
- Trust varies over time and the level of dynamicism may also vary between different relationships. For example, when I first starting partnering Bob in doubles I didn't trust in his every shot, now I trust almost all of his game (with the exception of his backhand so I make sure he plays in the forehand court as much as possible).
- Having a secured communications channel with another entity is never sufficient reason to trust that entity, even if you trust the underlying security primitives on which that communications channel is based.

Quite formally we can define trust as the level of confidence in the reliability and integrity of that entity to fulfil specific responsibilities. In more human terms Alice doesn't need to trust Eve if what Eve does has no direct impact on Alice. However if Alice needs to trust Bob and Bob has to trust Eve then Alice has an indirect trust relationship with Eve through Bob even though Alice and Eve may never be directly aware of this.

Fitting trust to a platform such as ITS is intrinsically complex. However trust is a major part of the transport problem. We choose one make of car over another because we may trust one to be more reliable than another, or we trust we'll get better service from this dealership rather than that one. We also may trust the train to get us to our destination with less stress than the bus, or driving. I may trust Campagnolo gears on my bicycle more that those from Shimano because I have a sneaking worry over a company making fishing tackle fiddling about with bikes (a silly fear really but trust is not meant to be rational). Too many times you can hear the statement "I trust him because he's got a nice face". Not rational. But it does drive our internal decision matrix.

The problem with trust in ITS is that effective trust requires identification—you need to know who you are trusting. So in a system such as C-ITS where most of the actors are unknown to one another we need to provide means for parties to build up trust. In trust networks this is achieved through delegated relational trust, in this case Alice needs to trust Bob but doesn't have a relationship with Bob, however Alice has a trust relationship with Eve and Eve trusts Bob. Bob presents Alice with some proof that Eve trusts him to Alice, and Alice if she accepts this proof

essentially delegates the trust decision to Eve. So although Alice doesn't establish a formal direct trust relationship with Bob she has accepted Eve's trust in him as sufficient and makes her own trust based decisions on the basis of Eve's trust.

It should be generally considered that delegated relational trust is weak. If the decision to trust or not to trust is always left to somebody else, there is no ability to build a true contextual trust model. However in cryptographic models used for trust often the model tends towards one of making an assertion, getting a mutually trusted third party to verify it, and then on the basis of what the mutual third party has verified, the relying party acts on the assertion.

For C-ITS in both the CAM and DENM models all the assertions in the message (location, time, identity, event) are self-asserted by an unknown party but the authority to make these assertions is transmitted as a cryptographically strong signed document.

10.4 Privacy

Privacy is quite unlike any other security problem where metrics of the degree of protection can be applied. For example, if a risk analysis identifies that there is a risk that a data object can be manipulated and that such manipulation should be detected it is possible to specify that the data is protected by providing a signed hash of the message which will meet certain conditions.

For C-ITS there are a number of occasions where data that can be considered personal is exposed across interfaces between the system components. One of the main areas of concern is that of locational privacy as C-ITS is based on regular updates of an object's location being broadcast to any party able to receive it and where there is no prior knowledge of who the receivers are. For the present time C-ITS is not fully deployed but it does share similarities with the smartphone and thus the quote from the Article 29 working group opinion on the use of GeoLocation data in the smartphone environment [2]:

> A smart mobile device is very intimately linked to a specific individual. Most people tend to keep their mobile devices very close to themselves, from their pocket or bag to the night table next to their bed.
>
> It seldom happens that a person lends such a device to another person. Most people are aware that their mobile device contains a range of highly intimate information, ranging from e-mail to private pictures, from browsing history to for example a contact list.
>
> This allows the providers of geolocation based services to gain an intimate overview of habits and patterns of the owner of such a device and build extensive profiles. From a pattern of inactivity at night, the sleeping place can be deduced, and from a regular travel pattern in the morning, the location of an employer may be deduced. The pattern may also include data derived from the movement patterns of friends, based on the so-called social graph.
>
> A behavioural pattern may also include special categories of data, if it for example reveals visits to hospitals and religious places, presence at political demonstrations or presence at other specific locations revealing data about for example sex life. These profiles can be used to take decisions that significantly affect the owner.

> The technology of smart mobile devices allows for the constant monitoring of location data. Smartphones can permanently collect signals from base stations and wifi access points. Technically, the monitoring can be done secretively, without informing the owner. Monitoring can also be done semi-secretively, when people forget or are not properly informed that location services are switched on, or when the accessibility settings of location data are changed from private to public.
>
> Even when people intentionally make their geolocation data available on the Internet, through whereabout and geotagging services, the unlimited global access creates new risks ranging from data theft to burglary, to even physical aggression and stalking.
>
> As with other new technology, a major risk with the use of location data is function creep, the fact that based on the availability of a new type of data, new purposes are being developed that were not anticipated at the time of the original collection of the data.

Quite simply all this says is that people are sensitive about people knowing where they are. C-ITS requires declaration of where you are and when, so the challenge is to allow this data to be declared without raising the sensitivity. The conventional approaches in technology to give assurances of security are relatively simple:

- Anonymity—ability to use a resource without revealing the user's identity
- Pseudonymity—ability to use a resource without revealing the user's identity but maintaining accountability for the use of the resource
- Unlinkability—a user may make multiple uses of resources or services without others being able to link these uses together
- Unobservability—a user may use a resource or service without others being able to observe that the resource or service is being used.

Of these only Pseudonymity has been fully exploited in C-ITS and takes the form of modifying the identity over the time the vehicle is moving. The intent of providing pseudonymity is to assist in providing privacy protection against a casual observer. There are some difficulties in providing full privacy protection in C-ITS as the vehicle you are driving is traceable back to you as owner or driver (this is a legal requirement), your vehicle is also a visible object on the road and the windscreen is transparent so obviously a keen observer will see you driving the vehicle. Section 10.5 considers identity in much more detail.

10.5 Identity and Identification in C-ITS

Transport, particularly for ITS, has raised lots of flags and worries regarding identity. I find this somewhat difficult to get to grips with and it is at the root of the privacy versus accountability debate. What I will try and outline here are cases where we can make the debate more open and thus understand the steps that have been taken in the C-ITS standardisation world (where I come from) to address both sides of the debate.

It is not possible in the bulk of the industrialised world to simply put together a vehicle in your personal workshop and to drive it on the road. Rather, a vehicle

is subject to a long set of tests and approvals before it is allowed on the road. On completion every vehicle is assigned a Vehicle Identification Number (VIN) which is mostly based on ISO-3779 [3] and consists of three parts:

- Manufacturer identifier
- Vehicle descriptor
- Vehicle unique identifier

This is not all that different from the idea and construction of similar identifiers used in mobile phones (the International Mobile Equipment Identifier (IMEI) in 2G/3G, the TETRA Equipment Identifier (TEI) used in TETRA). The VIN can be used to deter fraud and other crime involving the vehicle itself as the VIN is hard coded to the vehicle.

Vehicles are registered for use and this secondary identity is the one we see on the number plate. A large number of, mostly national, standards apply to the construction of vehicle registration numbers and there are standards on the colours used, the fonts and so forth in order to maximise visibility. The laws in most countries state that the vehicle registration number has to be visible at all times the vehicle is on the road. The registration process, in addition to giving the visible identity of the number plate, and making the association of VIN (specific vehicle) to registered vehicle, there is also the association of vehicle to its owner (in the UK it is termed "registered keeper"). In the construction of these identifiers the VIN is structured and managed to be unique, the vehicle registration is structured and managed to be unique. So there is a clear and managed 1-to-1 relationship between VIN and Registration-Id. Any registered keeper of a vehicle may have 1 or many vehicles under their ownership (but of course can only drive one at a time—unless the registered keeper is a corporation and I'll look at that shortly).

Since 1903 in the UK and Germany (only Prussia at the time) driver and vehicle licensing started to become mandatory, and by 1977 when Belgium succumbed and introduced a driving test, almost all of the industrialised world requires mandatory testing of drivers before allowing them to drive a motorised vehicle on the road. One of the results of licensing is the issuing of a unique driver licence identity (note that in some countries, e.g. Spain and Sweden, the driver licence number is the same as the citizen-id). At the root of the thinking is that drivers of vehicles have to be accountable for their actions, it is a crime to withhold the identity of the driver when requested to disclose it by an authority.

Thus we have three (at least) managed identifiers associated with any vehicle on the road:

- VIN
- Registration number
- Driver (licence) identity

The role of these identities in transport management is necessary to consider when we begin to explore the threats to them and in particular their misuse. We also need to consider the privacy angle.

In many cities and roads Automatic Number Plate Recognition (ANPR) is used for access control (more precisely for road pricing but the result is often access control—in order to access certain roads you have to pay a fee). In cities such as London where there is a congestion zone any vehicle crossing into the congestion zone has to pay a fee. The number plate is read by a set of cameras and the recognised number plate is used to determine if the appropriate fee has been paid. The driver has a set time to pay the fee and can do so in a number of ways—in all cases paying the fee against the number. However if the required fee is not paid the system can find the name and address of the registered keeper and make the demand for payment directly.

From a safety perspective each of these identifiers has a specific contribution to make: The VIN allows specific models of vehicle to be identified and specific instances of each model. This becomes important in issuing product recall notices and similar to assure the wider context of vehicle safety. The registration number is visually worn on the vehicle and is used in a number of contexts to control the behaviour of the driver. If a vehicle is seen to do something wrong and needs to be held to account it links to the registered keeper. As vehicles cannot (for now) be directly held to account for their actions it is the driver that is held to account and one of the responsibilities of the registered keeper is to identify who was driving the vehicle at any time.

All of these checks and balances through these identifiers happen in a largely observational system. That is a system where external observations and searches are required to link event to vehicle to registered keeper to driver.

Where ITS, and C-ITS in particular, changes the system is that the vehicle now makes assertions of its own behaviour. This changes a vehicle from not just displaying its registration number on the outside but also allows it to display other attributes on the outside of the vehicle. So prior to C-ITS and the use of regularly updated CAMs an external observer would have to take deliberate action to determine a vehicle's speed and trajectory. Now with ITS any similarly equipped observer can directly calculate the speed and trajectory of all the CAM transmitting vehicles in range.

The impact is now that vehicles, and their drivers, are self-asserting their speed and thus how close it is to the legal limit. Self-declarations of breaking the speed limit are open to prosecution and there have been a number of instances of drivers taking video of their illegal driving, posting them on YouTube, and then having the police knocking on their doors to prosecute. The evidence to prosecute has been self-asserted in the posted video and has the weight of a confession.

There are a number of difficult questions here and the difficult societal one is that of self-assertion of guilt. So there is a scenario in which when driving in an area with a speed limit of (say) 30 mph and you assert you are driving at (say) 35 mph then you are asserting that you are breaking the lawfully set speed limit. There is a line that breaking the law is simply that—breaking the law. If you self-assert you've broken the law, it doesn't change liability. The wider societal question is will you be

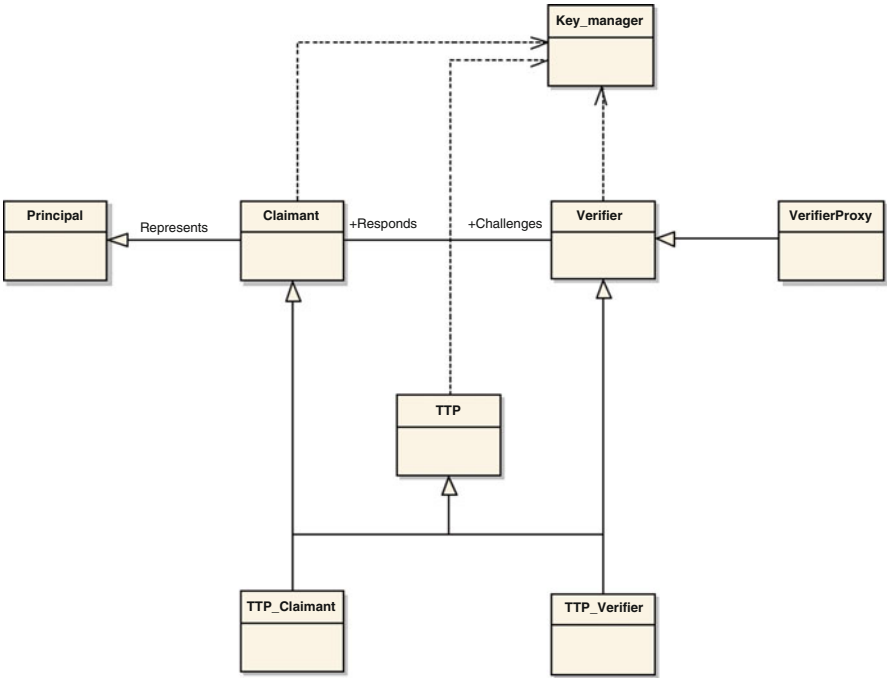

Fig. 10.4 Model for authentication

prosecuted for every self-asserted violation? Happily that is not something this book has to answer. However combining ITS with software control of vehicle dynamics there is no reason why vehicles can't assist drivers in staying legal.

The common security problem associated with identifiers is to masquerade as one. That is Alice claims to be Bob. In order to counter masquerade the security tool is authentication. In formal terms the party being authenticated is referred to as the principal. The entity that requires authentication of the principal is termed the relying party. The model for authentication is given in Fig. 10.4.

Authentication methods rely upon something the principal is, has or knows, where is, has, knows are considered as classes of information. Authentication that uses attributes from only one of these classes is called single factor authentication, and if attributes from two or more of the classes is used in the authentication it is referred to as multi-factor authentication (two-factor if attributes from two classes are used, three-factor if attributes from all three classes are used). The use of two attributes in a class does not make the authentication two-factor. Typically if a human is the principal he is identified by some form of biometric data and the assumption for authentication is that the biometric data is unique and not forgeable.

When the authentication factor uses something the principal has it often refers to a specific hardware module containing some unique and non-forgeable secret. This is the model used in Subscriber Identity Modules (SIM) cards where the key is

contained on the SIM held by the user's phone. The third case is where the user has to have knowledge and covers passwords, Personal Identification Numbers (PINs), and pass-phrases.

For all of the existing identifiers authentication is achieved using supporting authoritative documentation. The challenge in C-ITS (and ITS in general) is to first of all identify the principal and the relying parties.

In C-ITS the primary problem is that any pair of vehicles will not have any prior knowledge of each other thus there is no means to establish any credentials for authentication. However in C-ITS the relying party, i.e. the receiver of any CAM or DENM, has to be able to gauge the correctness of the data. So this means data claiming to be from a vehicle has to be verifiable as coming from a vehicle. Similarly data coming from a particular location has to be verifiable as coming from that location.

The role of authentication in C-ITS is inevitably complex. For much of the time we don't really care who you are, but we do care what you are. This means we want to be able to verify attributes and not identity. For example, I need to know you are a car and not a truck but don't need really to know exactly which car or truck. However if I want to determine the likelihood of a collision I do want to be able to link all your transmissions together and this means there has to be some time invariant uniqueness in your transmission (else if there are 20 or 30 or more transmitters all claiming to be cars and I am unable to distinguish one from another then I can't reasonably determine if any are going to collide with me).

10.6 Symmetric and Asymmetric Security

When technologists talk about security they often mean cryptography. Very simply cryptography is the mathematical means of providing security. Where cryptographic methods are used to support security the primary element of achieving security is in the key. The general assumptions for any system relying on cryptology are:

- Knowledge of how algorithms work is in the public domain.
- Knowledge of protocols for authentication and key establishment are in the public domain.

The only means of assuring security remains in place, over and above the known limitations of the algorithm and protocol, is in the secrecy of the key. A secret is by definition not a secret when it is widely known and so a shared secret is not really secret. Symmetric key cryptography works only by control of the number of entities who know the secret and generally, for telecommunications, the intention is to limit this to two parties only. However in public communication where secrecy may be required of communication to a large number of unknown parties the normal definition of secrecy cannot apply. The challenge of this is met by a set of techniques based on non-secret cryptology, or asymmetric keying, whereby a key has two components one of which is private and the other is public. The success is built

on the mathematics of the key construction and on the algorithms that make use of the key, but essentially it consists of a pair of one-way functions and the view that is computationally infeasible from knowledge of the public key to find the matching private key. A public key can then be distributed freely to either receive data encrypted by the private key, or to encrypt data to be sent to the holder of the private key.

In symmetric key cryptography there is one mandatory requirement:

- Only two parties have access to the key.

In order to maintain compliance with this requirement there are a number of approaches to key distribution that may be taken. In each case the key should be delivered in a manner that leaves an audit trail. In addition the key should be transmitted in a tamper proof format: tamper proofing may be achieved in either software or hardware. It has often been claimed that symmetric cryptography doesn't scale which can be comprehensively busted with the evidence of the 2G and 3G cellular networks. In this domain symmetric keys are distributed on smart cards (the SIM) and there are some seven billion keys distributed in this way with no known breaches of security. Furthermore the SIM is a tamper proof means of distribution that has been well tested over the years (the same basic form factor and technology is used in all smart cards thus in a very wide range of industries including banking). There are no asymmetric cryptographic key distribution networks of comparable size (the biggest reported PKI is that used internally to the US Department of Defence and has only three million subscribers) (Fig. 10.5).

In asymmetric cryptography a public key can be distributed to either receive data encrypted by the private key, or to encrypt data to be sent to the holder of the private key. However there is a legitimate concern that whilst the mathematical relationship is understood to work there is often only a weak relationship between the two communicating parties hence trust that the data is visible to the correct party has to be assured. The counter to the trust problem is to distribute public keys through a trusted source within public key certificates according to clause 7 of ITU T Recommendation X.509 [13].

A certificate is a signed data object that contains the data elements summarised as follows:

- The identifier of the certification authority.
- The unique identifier of the user of the certificate.
- Some attributes of the user, like address, company, tax code, etc.
- Public key, generated with the private key, to be used to verify digital signature.
- Period of validity of the certificate, defined by a start date and an end date.
- Unique identity code of the certificate.
- Digital signature of the certification authority.
- Environment in which the certificate is valid.

Certificate extensions can be used to provide authorisation as opposed to identification wherein the extensions provide methods for associating additional attributes with users or public keys and for managing the hierarchy.

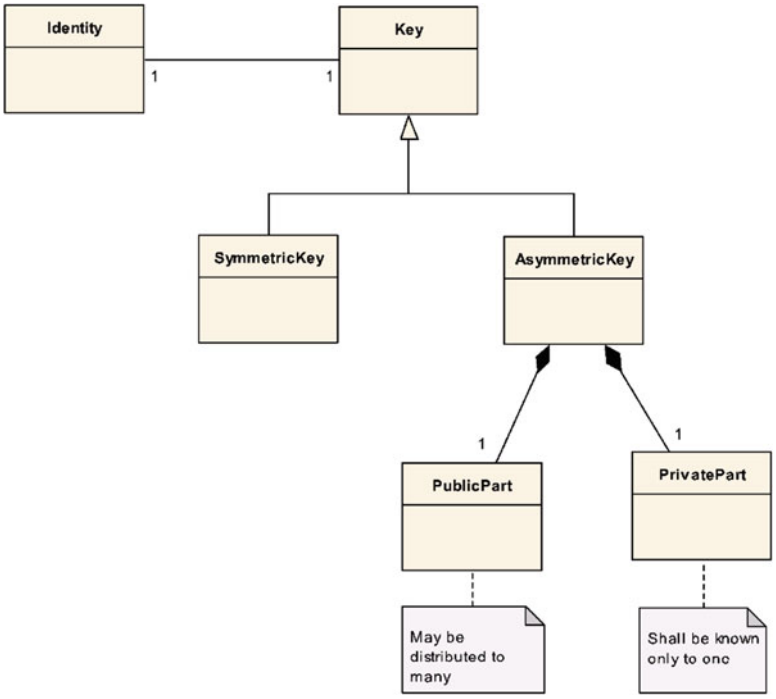

Fig. 10.5 Relationship of identity and keys

A Certification Authority (CA) is a trusted third party that issues certificates. In PKIs the CA verifies identity. CAs (certification authorities) can issue different kinds of certificates:

- Identity.
- Authorisation.
- Transaction.
- Time Stamp.

The standards developed to date (June 2014) provide both identity and authorisation certificates with more than one type of CA in order to give the possibility of pseudonymous operation.

10.7 Security Standards for C-ITS

The global C-ITS market is underpinned by common standards and in this regard the security domain is no different. There are essentially three bodies pushing in this domain:

- International Standards Organization (ISO) (mirrored in European Committee for Standardization (CEN))
- European Telecommunications Standards Institute (ETSI)
- Institute of Electrical and Electronic Engineers (IEEE)

In addition to these bodies there are a number of other parties working to bring C-ITS as a common framework to the market and key amongst these are the Car-to-Car Communications Consortium representing industry and the major Original Equipment Manufacturers (OEMs), the EU and US governments seeking harmonisation across the Atlantic, the International Telecommunications Union Telecommunication and Radio units (ITU-T and ITU-R) who alongside ETSI and the European Conference of Post and Telecommunications Administrations (CEPT) give guarantees of radio access, and there are increasing global standards agreements being developed by ETSI and others to ensure as far as possible that key areas, including C-ITS, have as far as is possible a single set of standards that give assurance of a global market for manufacture, distribution and operation for C-ITS. For a detailed overview of standardisation and harmonisation efforts, see Chap. 2.

The approach to security standards for C-ITS has been fairly conventional:

- Risk Analysis published as ETSI TR 102 893 [4]
- Security Architecture published as TS 102 940 [5]
- Security Countermeasure set published as TS 102 941 [6], TS 102 942 [7] and TS 102 943 [8]
- Data Dictionary for security published as TS 103 097 [9]

In addition these ETSI standards directly reference the IEEE 1609.2 [10] specification for certificate structures and cryptographic measures. Also all of these standards fit into the overall ITS-Station architecture [11, 12] as a set of security services. Graphically this can be seen in Fig. 10.6 which is consistent with the overall approach to risk management that is at the heart of this entire chapter.

The resulting standards that have been developed extend the basic architecture of the ITS Station by describing the application of security services across the stack. This is shown in Fig. 10.7.

In the more visual world this again mimics the core capabilities of C-ITS by mapping specific security services to C-ITS entities and transmission types. This is best shown in Figs. 10.8 and 10.9.

In the standardisation of C-ITS at ETSI and ISO/CEN all groups involved have selected 1609.2 as the core building block for security. Furthermore there is almost complete global acceptance of this selection with the resulting agreements on algorithms and key sizes. The global market is further enhanced by work being done to ensure that the core features have freedom of application and cross border use for C-ITS.

The IEEE 1609.2 standard defines secure message formats and processing for use by Wireless Access in Vehicular Environments (WAVE) devices, including methods to secure WAVE management messages and methods to secure application

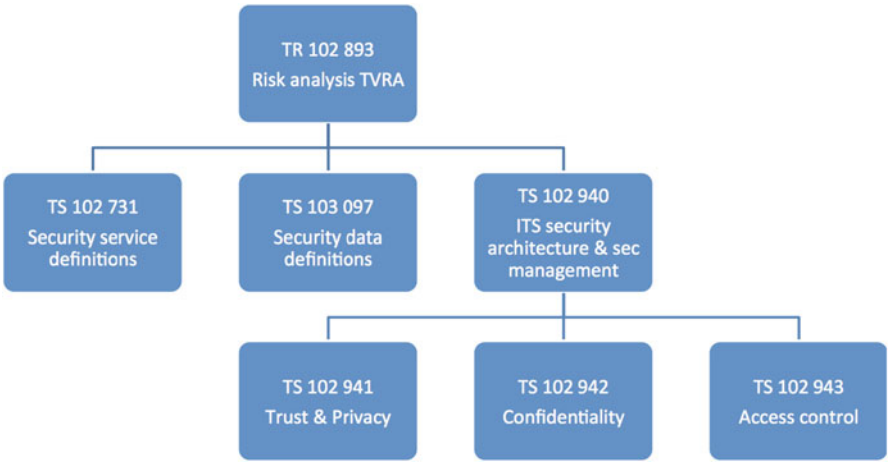

Fig. 10.6 The ETSI standards publications and their relationships

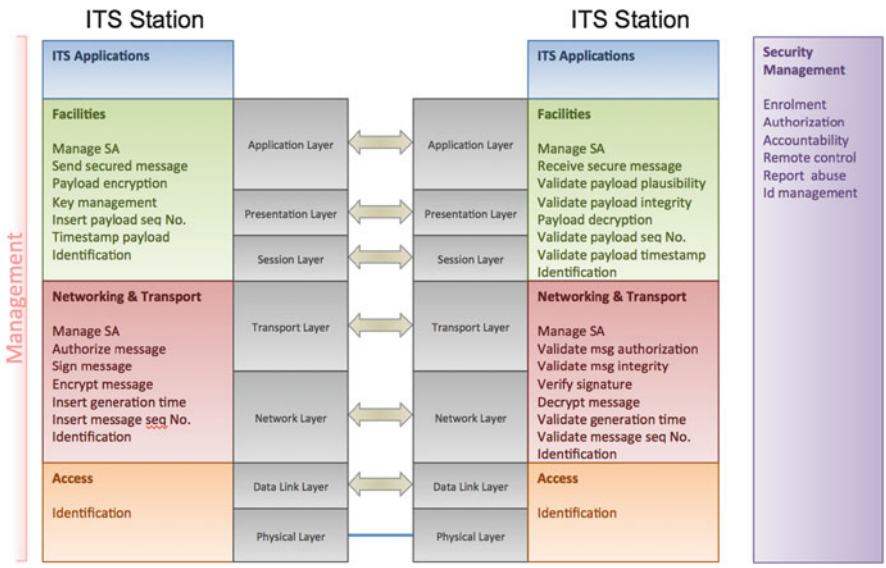

Fig. 10.7 Standardised security services mapped to the OSI protocol stack

messages. Fortunately the IEEE community has worked in close co-operation with ETSI and ISO to ensure that the security functions and features provided are not limited to WAVE and thus those other communities have looked to the 1609.2 capabilities as a toolkit for satisfying the authentication, integrity and confidentiality requirements for ITS in general and C-ITS in particular. Simplifying 1609.2 to its

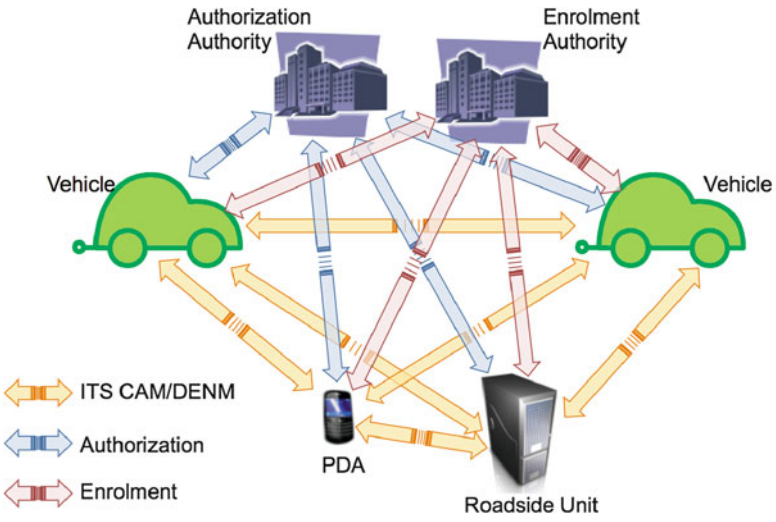

Fig. 10.8 Standardised security services mapped to the C-ITS entities

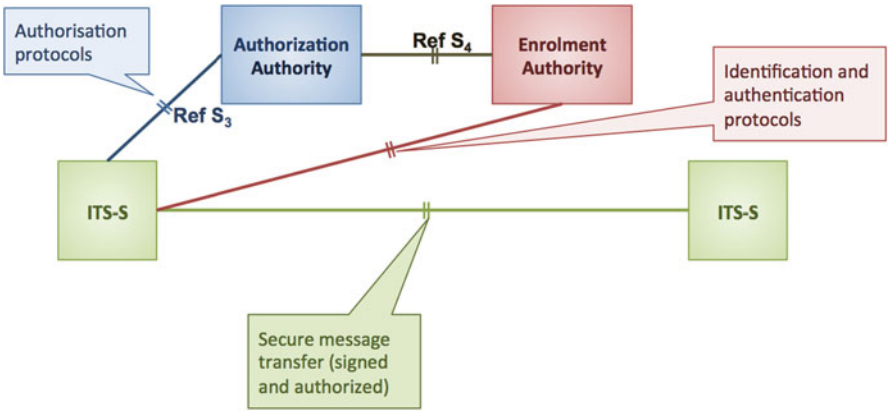

Fig. 10.9 Standardised security services mapped as functional reference points of C-ITS

core services is important as whilst 1609.2 has some novelty in its use of elliptical curve cryptography but that of itself is a natural choice (to give a cryptographic strength of 128-bits using a more conventional RSA[1] approach would require keys of 3,072 bits whereas with elliptical curve the keys are "only" 265 bits long).

[1]The approach taken by Rivest–Shamir–Adleman to public key cryptography based on the difficulty in factorising a given set of semi-prime numbers (a set of numbers that have as factors two prime numbers).

The security processing services of IEEE 1609.2 consist of the following:

- Secure Data Exchange
  - signing and/or encryption of Protocol Data Units (PDUs) prior to their transmission,
  - decryption and verification (as appropriate) of PDUs on reception.
- Security processing for security management
  - ensuring access to Crypto-material (private keys, public keys and certificates)
  - generating certificate requests and processing responses
  - validating Certificate Revocation Lists (CRLs)
- Storing private keys and their associated certificates.

The end result is that IEEE 1609.2's mechanisms provide support for the core C-ITS capabilities:

- Authorisation verification by certificate verification
- Confidentiality by encryption/decryption
- Integrity proof generation and validation

So in applying 1609.2 to C-ITS, for CAM say, the transmitting station chooses a key pair with a validated pseudonymity and authority public key certificate and signs the CAM prior to transmission with the matching private key. It then transmits the signed CAM (as a PDU or datagram) with the appropriate certificate such that any receiving party can validate that the transmitter did actually send the CAM and that he had authority to do so verified by a shared authority. In this case the application of 1609.2 is much like any other public key scheme with the cryptographic advantages brought by use of elliptical curve cryptography.

We have already looked at the general concepts of cryptographic security and the role of symmetric and asymmetric keying. However we now need to look more closely at what is involved in C-ITS and this requires us to specifically look at IEEE 1609.2 [10] and how it is involved in securing C-ITS.

A pseudonym, or alias, is an alternative identity. In C-ITS the identity given across the radio network is a pseudo-random identifier that is verified by a third party as belonging to an ITS-Station. The authority that does this third party verification doesn't much care which ITS-Station the identifier is attached to.

Every identifier is bound to a key pair and the public key is certified (by the aforementioned third party authority) as belonging to the identifier and the private key. When a package (a C-ITS message) is signed using the participant's private key it can be verified by any receiver holding the public key that it comes from a real ITS-Station.

When using identifier certificates in this way the transmitter is in control of how much they want to reveal of their identity by how often they change their pseudonym. However as each pseudonym has to be independently verified and every verification takes time this is a non-trivial calculation. In C-ITS the scheme used for

cryptographic signing is that defined in IEEE 1609.2 [10] and this offers a number of ways to ease the burden of creating multiple certificates from a single authorisation pass.

C-ITS uses the cryptographic certificate scheme defined in IEEE 1609.2 [10]. The cryptographic basis of this is elliptical curve asymmetric cryptography and for the application in C-ITS takes advantage of some of the capabilities of this branch of mathematics to allow autogeneration of new certified identities from a single authorisation.

The rate at which a pseudonym is changed is, as has been mentioned, a black art. It has to change often enough to act as a non-persistent identifier for the ITS-Station (and the vehicle it is associated with) but not too often that any ability of receiving ITS-Stations to determine the vector of movement of the ITS-Station and its associated vehicle. So every transmission is too often, once a month probably not often enough. This problem is not unique to C-ITS and has been faced by many other broadcast radio technologies including GSM and TETRA (Terrestrial Trunked Radio). In the former the unique user identity is exposed once at initial registration and then replaced with a temporary identity at every re-registration, in the latter the identity is similarly replaced with a temporary identity but in this case encrypted such that the value seen by a casual observer is different in every transmission with no means of correlation between values. The C-ITS approach is closer in spirit to the TETRA than the GSM approach but with the fine grain of control left to the transmitting station.

We often mention certificates and signatures, too often as synonyms. A digital signature is included in a certificate and represents a relatively simple process as shown in Fig. 10.10.

There has been a recurring question in the development of the C-ITS security model and that is: Where do you sign? By this it means at which of the protocol layers in the stack between two communicating ITS stations? Digital signatures sign documents and apply only to the document they sign. So we need to identify what is the "document" in C-ITS. The simplest view is that a CAM or DENM is the document—it is the statement prepared by the vehicle for sharing with other co-operating ITS stations. The signature applies to the completed document. So a CAM can be "signed" but only by the generator of the CAM. Given that CAMs are intrinsically mutable (i.e. for a moving vehicle each CAM will be different if the CAM is a statement "I am here now", so *now*, i.e. time, always changes and *here*, i.e. location, may change) and that the sender of the CAM has no prior knowledge of who will receive the CAM the sending station also needs to send the public key required to verify the signature.

The normal process of third party verification that a public key is bound to a corresponding private key is complex and often time consuming. This is a problem in C-ITS as time is in very short supply.

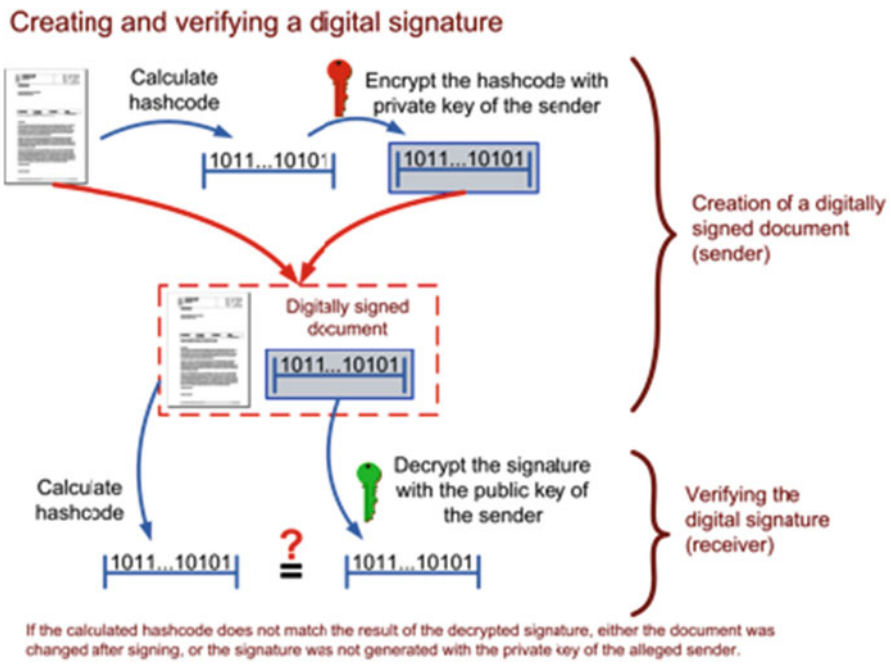

Fig. 10.10 The digital signature process

10.7.1 After the Standards?

The challenge that is still being worked through for global deployment of Secure C-ITS is in building the infrastructure of authorities that distribute the public key certificates. There are some opportunities afforded by the cryptographic mechanisms underpinning 1609.2 that allow for chains of key pairs to be spun off a single validated key pair can be used to advantage. This is important as with several millions of cars active on the roads of Europe at any one time where new key-pairs and certificates are required every few minutes it would simply be infeasible to have a vehicle connected to an infrastructure to go through a complicated and time-consuming certification process for a key that is only going to be used a few times before being discarded.

Beyond this there are other questions to be asked of standards and deployments. Amongst these are how to integrate C-ITS to other systems such as the smart city, to other geo-capabilities and to the inevitable changes in society that require acceptance of all vehicle types as needing to co-operate in ITS. This will need the ITS community to look at how to integrate the standards of today into alternative devices, the most prevalent of which is the smartphone.

10.8 Conclusions

Quite simply providing security in C-ITS is not trivial. The fact that Alice (the transmitting vehicle) and Bob (the receiving vehicle) have not got a previously established relationship, and Eve (the adversary of both Alice and Bob) has equal access to the data sent by Alice, makes any model that assures a secure link between Alice and Bob problematic. Adding to this is the problem that Bob is not necessarily an individual but may be a set of individuals whose only criteria to be Bob is that they are in range of the transmissions from Alice, and furthermore all Bobs are explicitly unknown to Alice.

For now C-ITS security is provided through a validated trust hierarchy. That hierarchy gives a limited degree of assurance that a vehicle is really a vehicle, that its claim to a particular role has been validated by a third party, and ultimately ensures that data received can be traced to its source. The trust model is enforced and reinforced using pseudonymous authorisation certificates following the models of IEEE 1609.2 and its underlying cryptographic model.

We cannot afford to be complacent regarding the security provisions in C-ITS and ITS in the wider domains. Serious efforts have been made to give assurance of global interoperability—all active C-ITS standards are based on a single common model for its cryptographic operations. Great efforts have been made in global standards to assure the industry works to a common set of standards and this is true for security as for other spheres of C-ITS. The long-term success of C-ITS requires that all the aspects discussed in this chapter are maintained.

Finally it is important to remember that security is a process and not a function. That process never stops.

Definitions

Access Control Policy
: A set of privileges representing access control rules that defines which allowed entities for certain operations within specified contexts each entity must comply with, in order to grant access to an object

agency
: Ability and opportunity of the individual to make independent choices

anonymity
: Act of ensuring that a user may use a resource or service without disclosing the user's identity

authentication
: Ensuring that the identity of a subject or resource is the one claimed

confidentiality
: Ensuring that information is accessible only to those authorized to have access

identity
: Set of properties (including identifiers and capabilities) of an entity that distinguishes it from other entities

impact
: Result of an information security incident caused by a threat and which affects assets

integrity
: Safeguarding the accuracy and completeness of information and processing methods

personal data
: Any information relating to an identified or identifiable natural person

privacy
: Right of the individual to have his identity, agency and action protected from any unwanted scrutiny and interference

pseudonymity
: Act of ensuring that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use

risk
: Potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the attacked system or organization

threat
: Potential cause of an incident that may result in harm to a system or organization

unlinkability
: Act of ensuring that a user may make multiple uses of resources or services without others being able to link these uses together

unobservability
: Act of ensuring that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used

vulnerability
: Weakness of an asset or group of assets that can be exploited by one or more threats

Acknowledgements The work reflected in this chapter has been supported by the i-SCOPE project, and by each of the SUNSHINE and i-locate projects and has incorporated some of the findings from the i-tour project.

i-SCOPE
: The project has received funding from the European Community, and it has been co-funded by the CIP-ICT Policy Support Programme as part of the Competitiveness and Innovation Framework Programme by the European Community, contract number 297284. The author is solely responsible for it and that it does not represent the opinion of the Community and that the Community is not responsible for any use that might be made of information contained therein.

SUNSHINE
: This project is partially funded under the ICT Policy Support Programme (ICT PSP) as part of the Competitiveness and Innovation Framework Programme by the European Community

i-locate
: The project has received funding from the European Community under contract number 621040

References

1. ETSI TS 102 165-1: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis
2. Article 29 of Directive 95/46/EC Working group Opinion 13/2011 on Geolocation services on smart mobile devices, Adopted on 16 May 2011
3. ISO 3779: Road vehicles - Vehicle identification number (VIN) - Content and structure
4. ETSI TR 102 893: Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)
5. ETSI TS 102 940: Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management
6. ETSI TS 102 941: Intelligent Transport Systems (ITS); Security; Trust and Privacy Management
7. ETSI TS 102 942: Intelligent Transport Systems (ITS); Security; Access Control
8. ETSI TS 102 943: Intelligent Transport Systems (ITS); Security; Confidentiality services
9. ETSI TS 103 097: Intelligent Transport Systems (ITS); Security; Security header and certificate formats
10. IEEE STANDARD 1609.2-2013 IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages
11. ISO 21217:2014: Intelligent transport systems Communications access for land mobiles (CALM) Architecture
12. ETSI EN 302 665: Intelligent Transport Systems (ITS); Communications Architecture
13. ITU-T Recommendation X.509: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks