Securing Digital Evidence

Jennifer Richter
Technische Universität Darmstadt
Germany
jenrichter@gmx.de

Nicolai Kuntze, Carsten Rudolph
Fraunhofer Institute for Secure Information Technology
Darmstadt, Germany
{nicolai.kuntze|carsten.rudolph}@sit.fraunhofer.de

***Abstract*—Non-repudiation of digital evidence is required by various use cases in today's business cases for example in the area of medical products but also in public use cases like congestion charges. These use cases have in common that at a certain time an evidence record is generated to attest for the occurrence of a certain event.**

To allow for non-repudiation of such an evidence record it is required to provide evidence on the used device itself, its configuration, and the software running at the time of the event. Digital signatures as used today provide authenticity and integrity of the evidence record. However the signature gives no information about the state of the Measurement Instrument at the time of operation. The attestation of the correct operation of the evidence collector is discussed in this paper and an implemented solution is presented.

Keywords: Reliable digital evidence, trusted computing

I. Introduction

The penetration of computers or other electronics into daily life increasingly influenced laws and jurisdiction the last years [16]. Evidence, especially paper-based evidence, like that used in courts is no longer the only kind of evidence used. Through the development of computer based technology, the importance of digital evidence like measured values, photos, or videos has increased. All evidence must meet certain legal requirements before being produced in court. Braid [3] defined five rules of evidence in order for evidence to be considered useful. Evidence must be admissible, authentic, complete, reliable and believable. However, digital evidence in particular must be regarded sceptically since it only exists in a binary representation. Without adequate protection mechanisms such data can be easily manipulated without leaving any traces. The collection, the handling, the storage and the presentation of digital evidence has met some problems in the past. Thus, courts now should demand stringent requirements on the admissibility of digital evidence at trial. As a result, digital evidence requires appropriate methods to prove and preserve their significance. Different countries have different laws. Therefore, restrictions on how digital evidence can be collected and used for court proceedings vary from each country. The collection of evidence can be significantly complicated by laws. On example are laws that affect monitoring and collection of digital information in the U.S. [19]. However, the protection of the integrity of digital evidence is only one part of the story. In addition, it is necessary to also regard the situation in which data was initially collected. Usually, a computational device is needed to produce digital evidence. Manipulated devices can produce arbitrary or malicious data. A variety of parameters of a device's state can be relevant for different types of evidence. Among others there is the executable software on the device, hardware used to collect evidence, software and hardware configuration, the exact location of the device, environment parameters like temperature or humidity, or the correct time of data collection. To reliably report these parameters and bind them to the collected evidence is a non-trivial task that touches a number of open IT security issues. This paper discusses one particular application and proposes one approach to deal with some of the open issues in this particular application.

The practical application considered here is concerned with the introduction of various kinds of Traffic Monitoring Systems (TMS). In almost every European country, automatical control of vehicles for exceeding speed limits, or tracing car movements for accounting the use of toll-roads is considered an acceptable practice. Traditional charging methods like badges and taxes are not appropriate anymore since the traffic load has increased substantially. The traffic load and the amplified environmental pollution require new charging schemes. In England, congestion charging schemes were developed to decrease the amount of cars driving through inner city areas, most notably the city of London [2]. In Germany, satellite-based and distance oriented truck tolls were discussed and implemented in 2005 [10]. Additionally, the Netherlands is currently discussing the introduction of a road fee for all public roads. In December 2007, the Dutch government decided to introduce a national road toll. In July 2008, parliament voted this toll into law. Apart from congestion charging and intelligent vehicle tax, monitoring the speed limit using digital evidence is already used but seen very sceptical with regards to privacy. In addition, the current practice of random samples seems not to be sufficient to motivate changes in driving behaviour. Speeding accidents increase while traditional techniques at reducing them do not seem to discourage drivers. Drivers, knowing the location of fixed speed measuring instruments, slow down in this area but accelerate right after they pass the instrument. Therefore, new techniques must be found to control speeding. One example is the distance based calculation of speed where vehicles must be identified at the beginning and end-point of a particular distance. One central factor in such systems can be the use of small and relatively cheap digital cameras with centralised monitoring instead of the current practice where people have to control the cameras and manually collect the evidence (e.g.

in the case of analog film or digital without communication channels).

This new method needs new data processing techniques to handle the arising amount of data. Particularly, the privacy of personal data as well as the integrity and the authenticity of such devices are a concern. Moreover, Blythe said 'the lack of appropriate technology will not be the constraint in implementing road-use charging in the near future' [2, page 356].

This paper presents the design of an embedded system that is able to collect admissible digital evidence through an automated process. The measurement process is mainly performed by a machine and human collection is kept to a minimum to ensure automation. For digital evidence to be admissible in a court of law in future, the system must be secure and the data produced must have integrity and authenticity. Furthermore, evidence records must be strictly bound to evidence showing the state of the system at the time of collection. This process must be done automatically since the system will not have any human inputs. Consequently, a shielded environment must be created to enforce the high restrictions courts should place on admissibility. This environment must have security functions that increase the protection of the collected digital evidence. Moreover, additional security information that attests the trustworthiness of digital evidence is produced to provide for admissible digital evidence.

Trusted Computing (*TC*) as defined by the Trusted Computing Group (*TCG*) is aimed to provide a Trusted Platform that can attest to its current configuration to a third party. The functionality behind is a Trusted Platform Module (*TPM*) and the platform hosting the TPM. We use this functionality to provide trustworthy digital evidence collected in an automated process. Digital evidence like measurements, photos, or documents is not seen as trustworthy since it is only existent in binary representation. Therefore, modifications and tampering of the collected data is easy but also hard to detect. With the help of TC, using the TPM as a hardware based root of trust, additional information can be created and added to the collected data to achieve non-repudiation of measured data in a court of law. During a subsequent verification of collected data combined with the additional security information shall prove that a certain event has happened at a particular time and location by a device in a particular state and that data was not manipulated later.

The outline of this paper is as follows. Section II introduces the intended use case. A brief security analysis is given in Section III. Section IV gives a brief introduction to those parts of TC technology that are relevant for the concept and the implementation. Section V describes the conceptual design of a secure environment aiming to provide non-repudiation of digital evidence.

II. Use Case

An automated process is used to collect different measurement data which later can be used for several analyses. Particularly, an embedded system is designed for measuring traffic data. The embedded system should contain functionalities that can be used to collect and report different kinds of traffic information.

The traffic measurement device shall be able to collect different kinds of Measurement Values (MVs) like infrared pictures, digital pictures, time value, speed value, number of vehicle, type of vehicle, location value, distance a vehicle covered, or traffic volume value as they are discussed in [4]. In praxis, there will be specialised systems with limited functionalities to save costs and to increase the systems performance. However, considering a large variety of MVs the design can be adopted to multiple fields of application. Examples are speed measurement, toll systems, congestion charging schemes, or traffic analysis e.g. with respect to calculating the number of vehicles or determining the period of time of most traffic. Also the differentiation of different types of vehicles (for example trucks) is a valid application [26].

For the security of the complete system it is not sufficient to consider only the devices and technical components itself. All different entities and processes involved are relevant. For example the production process and possible certification and initialisation processes need to be included into security considerations.

From the organisational point of view on such a system it is essential to define the involved roles and their interactions for a sufficient understanding of the overall system. We can distinguish following roles can be distinguished. The **manufacturer** produces the Measurement Instrument (MI) and delivers it to the provider. It is to be noted that the manufacturer is responsible for the correct operation of the meter and the initial gauging.

The **provider** can be seen as an technical integrator creating a functional system from the components from different manufacturers. When the MI is ready for use, the provider places the system to the operators' disposal. It may also be the provider's responsibility to provide certification and support archiving and evaluation of measured data. (respectively, an Archiving and Evaluation Unit (*AEU*)).

The **operator** controls the MI system. His responsibility is operating the whole system and evaluating its outcome. Regarding the value creation chain the operator is the entity interested in the overall functionality of the system. He must take care that storage conditions appear to be appropriate. Data can be rendered unreadable if it was stored for example unprotected from humidity, extreme temperatures and strong magnetic fields [16]. In addition, the operator can provide an expert for court who presents the results if necessary. This expert must deliver expert evidence about facts from the domain of their expertise and with primary duty to the court [25].

Out of privacy reasons, a **Privacy Certification Authority (PCA)** provides functionalities to supply privacy on the one hand and traceability on the other. This entity needs to be considered separate from the operator to fulfill the role of a Trusted Third Party for both sides, operator and citizen.

A **timing authority (TA)** offers a reliable time source for

all MIs deployed. In many cases public available time signals such as the well know DCF-77 signal is used [24]. Due to the fact that these systems do not provide for tamper protection or proof of authenticity additional means are required. It is to be noted that not all of these roles are inevitably be separated in all cases. Depending on the system architecture additional roles can be defined. For instance, a charging unit or billing unit surely would fit into the design of a toll system.

III. Security analysis

For the automatic collecting and presentation of digital evidence e.g. at court security goals have to be warranted. Otherwise, the collected measurement data will be useless as evidence. According to Patzakis [21] the digital chain of custody must always be warranted. Depending on the particular use case, security goals are associated both with the measuring or the editing and conversion processes. The general process described here is independent from the details on the actual measuring sensor and data formats. Furthermore, if MVs need to be converted and changed for evaluation it might be necessary to either record and protect raw data as well as converted data and the evaluation results. Figure 1 illustrates the system processes with assigned security goals.

Non-repudiation is the overall security goal. Measurement data must be collected in such a manner that in a dispute (e.g. at court) its trustworthiness cannot be argued. Non-repudiation is not one autonomous security goal but a combination of several security goals including integrity, authenticity, time, and optionally privacy. Since non-repudiation cannot be warranted without these security goals all of them must be respected. Confidentiality, availability and accountability are not relevant for non-repudiation. For the reliability and assurance of evidence data these additional requirements are not central. Nevertheless, secure solutions for collection and storage of digital evidence need to satisfy also these secondary security goals.

Integrity is the protection against unauthorised and unnoticed data modification. Vanstone et. al. [17] defined digital integrity as, 'the property whereby digital data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source'. In designing a TMS, the main requirement is that evidence records must be protected such that changing any parameters of the measured data cannot happen undetected.

Authenticity has several dimensions in the context of measuring and storing digital evidence. First and most important, in combination with integrity it is necessary to authentically bind measured data to a particular (secure and unmanipulated) device with all relevant parameters. Furthermore, authenticity of actions of human beings involved in the processes can also be relevant. This includes an assertion on the system state to document the behaviour of it.

Time can be relevant for many applications. The exact time of a particular actions, e.g of the the measuring and production of evidence records, needs to be tightly bound to evidence records. Reliable time stamping can ensure that an event definitely happened at a specified time and (combined with integrity) can assure that data has not been altered since the time it was created.

Privacy is the protection of personal data. No personal data shall be acquired by someone not allowed to view or collect this data. In the context of TMS' especially the risk of tracking individual citizens and their actions is to be considered. As privacy will not be the main focus of this publication it is to be highlighted that the local processing of user related data is one possible solution to prevent the accumulation of privacy relevant data at a central entity.

Confidentiality is the protection against the unauthorised acquisition of information. This point is more general but closely related to the privacy security goal. The the focus of this publication is on the non-repudiation of MVs confidentiality will only briefly discussed later on.

Availability is the protection against unauthorised impairment of the functionality of a component or system. For example, a system shall be protected against Denial of Service attacks, i.e. the malicious prevention of the production or storage of evidence records.

Accountability is similar to non-repudiation but including the responsibility of people for a particular action. The focus hereby is the association of the actions in a system and the entities causing the action.

The focus here is on the main goal of non-repudiation of evidence records, i.e. on the process to produce evidence records in a way that it is clear that they where retrieved in a correct (uncorrupted) environment on measurement devices with secure configuration. High assurance for non-repudiation of the measured data is based on two key ideas. The first essential part is to design a secure environment which meets the defined security goals such that measured data can be considered to correctly represent the actual situation. The second part is to add all relevant parameters to the measured data. Some examples of additional security-relevant information are

- the location of the device
- the identity of the device
- the time when MVs were recorded
- and the status of the system in terms of the running software and the configuration of it.

All information, MVs and security data, are stored in a specially created structure called Measurement Record (MR). To add another security level a digital signature is applied on the Measurement Records. The design presented in the following sections uses a Trusted Platform Module to digitally sign the MR with a specially created key that shall never leaves the protected environment in clear-text. Furthermore, the signing key can be bound to particular states of the device such that the key cannot be used when the device has been manipulated. The signed data is then ready for transmission to the AEU. It should be noted that TPMs cannot provide unconditional security. Physical attacks on the chip can reveal the secrets stored on the chip. A TPM is not tamper-proof. Nevertheless, a TPM can be considered tamper-evident. Thus, physical manipulations are always visible on the device.

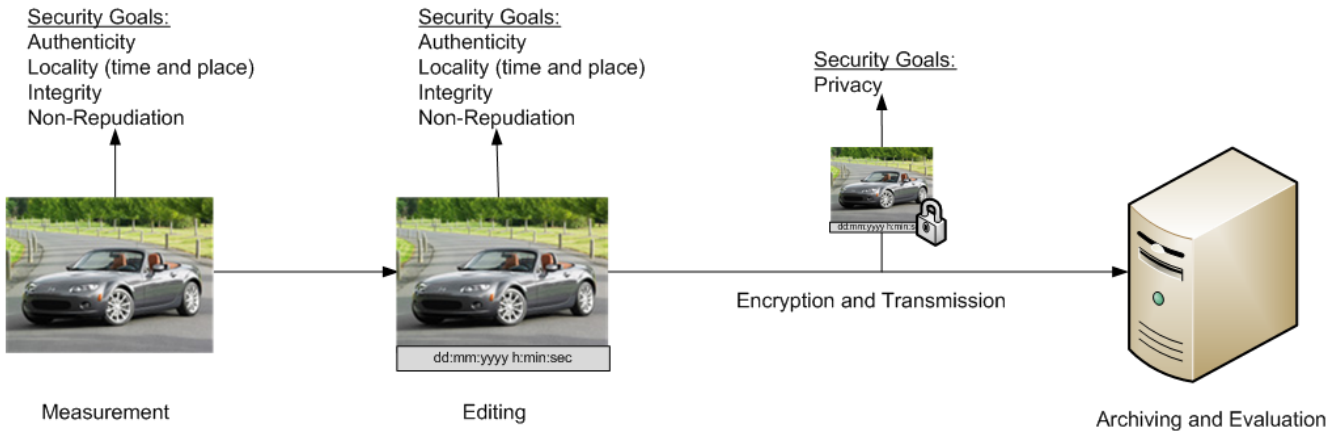

Fig. 1. Overall concept for the protection of digital evidence during the generation on the Measurement Instrument

Furthermore, such attacks need to be targeted on a particular device and require a large effort and high expertise. A much bigger concern are software attacks, that can be executed from remote and also be distributed to a large number of devices.

In the following section the underlying technology, the so-called Trusted Computing, is introduced as an approach to hardware based security. From the large different functionalities of the TPM those major elements are highlighted that are later used in Sections V and VI to address the security challenges presented. Readers familiar with Trusted Computing and TPM functionalities can skip the following section.

IV. Trusted Computing Essentials

The idea of building security into open, connected systems by using computing platforms enhanced by security-relevant functionality in protected places has a long history, rooted for example in early security requirement assessments as documented in the study by the Rand Corporation [1].

As shown in Section III protection of the identity of the device for evidence collection is an important security requirement. Furthermore, the lack of control on the physical access to the node induces strong requirements on the protection level. One possibility is to root security mechanisms in strong hardware security anchors. Trusted Computing [18] offers such a hardware root of trust providing certain security functionalities that, if combined with adequate hardware protection mechanisms, can be sufficient for achieving the required protection level. In this section these functionalities are introduced.

TC as defined by the Trusted Computing Group are computer systems extended by additional components which shall bring trust to the computing environment. Trust means that components of the system always work as implemented. To achieve this goal, the TCG has published and is still working on specifications describing architectures, affecting system components at any level from hardware to the operating system.

The TCG is the main industrial effort to standardise TC technology. Trust as defined by the TCG means that an entity always behaves in the expected manner for the intended purpose. The trust anchor, called Trusted Platform Module, offers various functions related to security. Each TPM is bound to a certain environment and together they form a Trusted Platform (TP) from which the TPM cannot be removed.

Most important hereby is the specification of the TPM. This module is mostly realized as a hardware chip hardwired to the computer platform. The current version of the TPM implements basic cryptographic functionality like SHA-1 calculation [8], message digest creation, random number generation, creation of 2048 bit RSA key pairs, and a RSA engine for encryption and signing purposes. Realized as an independent hardware module, it can provide protected capabilities allowing to shield secret data efficiently. This implementation also allows for in depth testing and validation of the soft- and hardware. The TCG defines three different roots of trust. These are components on which the trust to the whole system is built on.

The Core Root of Trust for Measurement (CRTM) [22] is implemented e.g. as an extension of the BIOS. Its duty is to perform measurements of system components involved in the boot process. Measured components then can perform measurements of other components involved in the next stage of booting. Through this principle of transitive trust, trust in the correctness of the measurement values can be passed on to the OS and the software executed in user space. All components together form a so called Trusted Building Block (TBB) if all components are measured. Through this architecture it shall be guaranteed that a computer system always starts in an authenticated state that can be verified by an external entity and therefore to spur the establishment of trust.

The second root of trust is the Root of Trust for Reporting (RTR). One of the aims of TC is to enable computer systems

to proof to other platforms that it is in a trusted state. Therefore the results of measurements of system components have to be presented to the remote platform. To guarantee the genuineness of these data, they are signed. For this purpose every TPM contains a 2048 bit RSA key pair, the Endorsement Key (EK), which is generated before shipping. The EK, together with an EK Credential, represents the identity of the platform. Pseudonymous representatives of the EK, so called Attestation Identity Keys (AIK) are used for signatures, for example of measurement results used by the remote party to verify the correctness of the desired state (Remote Attestation or Direct Anonymous Attestation) [5].

The third root of trust is the Root of Trust for Storage (RTS) with the purpose to establish a secure storage for cryptographic keys and other sensitive data. The RTS is implemented by introducing the Storage Root Key (SRK), a second 2048 bit RSA key pair stored in the non-volatile memory of the TPM. The SRK never leaves the shielded location of the TPM. That allows building a hierarchy of keys, with the SRK as the root, in which direct successors are protected by encryption with the SRK. These keys on their part can protect any number of other keys. Thus, trust is bequeathed from the SRK. Any key, following up the SRK can be stored off-chip, not least because memory in TPM is limited, but the number of possible TPM-generated keys is not. Keys never leave the TPM in clear; they are always encrypted by parent keys. The benefit from this is the possibility to work with encryption keys, which in the end are under protection of a hardware module and with this the possibility to encrypt data based on a hardware module. These keys allow to bind data to a device or even to a particular state of the device.

To prove trustworthiness of a TP to an external party, or verifier, processes called (remote) attestation and according protocols have been envisaged. They transport Measurement Values and data necessary to retrace the system state from them, so called measurement logs, to the verifier. The data is uniquely and verifiable bound to a particular platform, e.g. by a digital signature. Remote attestation can be supported by a PKI structure for instance to protect a platform owner's privacy by revealing the platform identity only to a trusted third party. The following technical details are taken from [29], more can also be found in [12] .

For the TPM to issue an assertion about the system state, two attestation protocols are available. As the uniqueness of every TPM leads to privacy concerns, they provide pseudonymity, resp., anonymity. Both protocols rest on Attestation Identity Keys (AIKs) which are placeholders for the EK. An AIK in the current version of the TPM is a 1024 bit RSA key whose private portion is sealed inside the TPM. The simpler protocol Remote Attestation (RA) offers pseudonymity employing a trusted third party, the Privacy CA (PCA), which issues a credential stating that the respective AIK is generated by a sound TPM within a valid platform. The system state is measured by a reporting process with the TPM as central reporting authority receiving Measurement Values and calculating a unique representation of the state using hash values. For this, the TPM has several Platform Configuration Registers (PCR). Beginning with the system boot each component reports a Measurement Value, e.g., a hash value over the BIOS, to the TPM and stores it in a log file. During RA the communication partner acting as verifier receives this log file and the corresponding PCR value. The verifier can then decide if the device is in a configuration which is trustworthy from his perspective. Apart from RA, the TCG has defined Direct Anonymous Attestation. This evolved protocol is based on a zero knowledge proof but due to certain constraints of the hardware it is not implemented in current TPMs.

AIKs are crucial for applications since they can not only be used, according to TCG standards, to attest the origin and authenticity of a trust measurement, but also to authenticate other keys and data generated by the TPM. Before an AIK can testify the authenticity of any data, a PCA has to issue a credential for it. This credential together with the AIK can therefore be used as an identity for this platform. Using the AIK as a signing key for arbitrary data is not directly possible but we have shown elsewhere how to circumvent this limitation [12].

V. Concept

Digital evidence can be vulnerable to manipulation or damage of records between the time they were created and they are used as evidence [16]. Further, they can already be corrupted at the initial recording. Therefore, the goal is to create a secure environment for the automatic collection, storage and transmission of measurement data. Later, the measurement data together with the information on the platform status and other parameters shall be used as digital evidence in court.

Software based techniques have proven to be vulnerable to various kinds of attacks and failures. In the context of collection of legally valid evidence such attacks and failures obviously threaten the security of produced measurements. Software solutions are more easily modified and manipulated than their hardware equivalents. Pure software solutions on standard hardware can be advantageous in terms of costs, easy development and maintenance but it can also be disadvantageous because of their ability to be compromised. In contrast, hardware based security solutions are considered to be more secure since physical access can be required for successful attacks. For example, code burnt onto a hardware chip cannot be easily modified to malfunction or leak critical data. Additionally, software is usually weak in providing appropriate storage capabilities for keys. Hardware solutions burn keys into the hardware or store them in non-volatile storage made inaccessible with other hardware means. Both methods make it difficult to circumvent the protection mechanisms also implemented in the integrated chip.

In general computing systems are highly complex architectures with a lot of heterogenous software and strong changes to the operational state e.g. by software updates or various different purposes. Therefore, in general it is not possible with current technology to derive from a measured system state any

well-founded statements on the overall security of the device. In contrast to the general case, use cases like Traffic Monitoring Systems have a well-defined purpose and only require a restricted set of software. With proper development and testing the state of the software might even be stable for long time periods. Further, there is no need for dynamic changes of their system functions. The relatively low complexity of the specialised use case allows for the beneficial application of Trusted Computing to get reliable security statements.

Hardware based security functionalities can increase the level of confidence in order to fortify the probative force of secured and stored evidence. Trusted Computing as introduced in Section IV offers a strong unique identity and also certain reporting functionalities to authenticate the behaviour of the device. The TPM serves as a security anchor for the device and provides relevant security mechanisms. From the TPM functionality digital signatures, hash values, time stamping and the secure storage function are used.

In addition to the TPM itself, a secure system environment is required for the accumulation and processing of measurement data. The collected Measurement Values shall provide enough information so that it is indisputable that a particular event happened as represented by the collected data. Thus, an environment must be created in a manner that detects and reports any alterations done to it and its created evidence. Alterations are detected in comparing pre-defined trusted system states to the state at the time of data collection. Note that it must be impossible to change data collected on a correct system even when the system has intermediate phases where it was in a corrupted state (again excluding physical attacks).

The secure environment has to offer certain means to report the status of a system. As integrity of the running system needs to be proven at all times, especially, to an external entity such as a reviewer or an expert at court.

Furthermore, the system status strongly depends on the boot process. A system that is already booted into a malicious state cannot yield adequate trust in a court of law. Therefore, a trusted boot process is required. In addition, protected means are required to securely store the representation of the system state. Undetected alterations to the system state may lead to a faulty running system. Furthermore, cryptographic keys should be used to help protect the system. The creation, usage and storage of private keys carry some risks as the whole value of the evidence depends on the level of protection of these keys. Thus, protected means for private keys are required. Section V-A presents the brief description of the minimal steps of the process. In Section V-B the architecture of a secure evidence collector is presented. The extensions to the roles given are introduced in Section V-C. It is to be noted that processes, architecture, and roles are different views on the overall concept and therefore depend on each other.

A. Processes

Based on the presented generic use case of Measurement Instruments the production and initialisation, deployment, use, and maintenance steps can be distinguished to define the life cycle of the individual MI. In this section these four steps are examined with respect to security requirements and the presented overall concept. Hereby, it is to be noted that we disregard revocation of a specific MI in this description. However, in practical realisations it is necessary to revoke certificates belonging to physically manipulated devices.

Production and initialisation is performed by the manufacturer and consists of the development of hardware and software components. During production of the hardware components the manufacturer integrates TPM and platform in each product for delivery. It is assumed that TPM and platform are shipped with certain credentials stating the conformance of these components to standards and requirements. The manufacturer certifies the integration through the issuing of a credential in form of a certificate. Software components used by the Measurement Instrument also need to be certified using special credentials issued by the manufacturer. These software credentials are known for example in the mobile domain as Reference Integrity Manifests [9] and testify that a certain software fullfils the requirements and is fit for use.

Given that hardware and software are well built and certified by sub-contractors and manufacturer, software is installed and initialized according to the requirements of the underlying use case and deployment strategy. One important step during initialisation is the creation of keys. It depends on who is taking which responsibilities in the process and also needs to be adapted to particular deployment processes . One possible scheme is that activation of the TPM (take ownership) is already done during initialisation by the manufacturer. Then, the manufacturer can create a first AIK and get a certificate from a privacy CA. The privacy CA could also be offered as additional service by the manufacturer. Also additional keys may be created e.g. to set up security modules like hard disk encryption or to protect certain critical values stored.

Finally, reference values are created representing the state of the Measurement Instrument including hard- and software. These reference values are then certified by the AIK created before. This process could also be deferred to a later process. The advantage to create the AIK during production and to certify the device at this early point in time is that the manufacturer can execute these first critical steps in a protected area without malicious interference. Solutions to address this challenge during deployment are more complex and therfore expensive.

Deployment can be executed by a provider or directly by the owner and operator of the MI. Installing it in its target environment needs to respect properly defined procedures for the installation. Part of the procedures for the installation cover the operation parameters like orientation, location, or temperature range. This task is documented recording the device id, person responsible, location, date, and time as a minimal set of information. After the physical installation communication with the central entities for the provision of relevant services like the date and time is established an tested. This communication is already part of the logs by the central entities. Finalisation is documented by a set of reference values

generated by the MI including the Measurement Values of the system state. This first set of measurements is archived in case a later examination and proof for correct deployment is required.

Usage of the MI covers system boot and synchronisation of the local time for the start up, evidence collection and potentially conversion and evaluation, signature, and evidence record transfer to a central entity as part of the intended application. During the boot process all software components and hardware configurations need to be measured and recored in TPM platform configuration registers in order to enable the attestation of the current system state. In the operation of the system, one can distinguish *authenticated boot* and *secure boot*. Authenticated boot provides Measurement Values but does not enforces the correctness of the software to be started. Secure boot enforces the integrity of the boot process by interrupting the process in case of changes software or configuration. Therefore, in the case of secure boot the boot process either fails or ends with a system running in an expected state. Secure boot prevents the collection of evidence in insecure system states. Thus, for strong privacy secure boot can be required. Securing evidence can also be realised with authenticated boot. Another approach can be cumulative attestation as introduced by Gunther et al. [14], [15]. However, currently only authenticated boot is available for most platforms. After boot, the local time of the MI needs to me synchronised with a real time clock. The local time needs to be protected by adequate means against tampering but needs to be local to ensure functionality also in an independent (offline) operation.

During operation sensors can monitor physical parameters of the operating environment. Operation policies might restrict the correct operational state to particular parameter ranges (e.g. very low temperature might change the behaviour of the system). This information is then combined with actual measurement data, and signed and time stamped stating the origin, integrity of data and instrument state, and creation time of the evidence. Such an evidence record is first locally stored. Special additional information can be embedded into the signature to also provide evidence on the completeness of the record in total, e.g. by a running counter. The final transfer to a central entity for evaluation of the evidence records is done as a deferred step. Existing security protocols can be used to protect this transmission.

Maintenance is required to maintain the correct operation of the Measurement Instrument.One regular task usually is the update of the software due to different reasons as for example bug fixes or improved functionality. Such a software update leads to a change of the state of the system resulting in e.g. keys that are not accessible any more as they are bound to the original state of the software. A migration scheme is required to allow for this procedure.

Due to e.g. gauging reference, parameters may change from time to time for example as a result of the aging of the hardware sensors. Changes to the operational parameters are also part of the system state and need also a certain reaction scheme to guarantee operation. Both schemes require a proper documentation to ensure the probative force of the evidence records collected after the change. Hereby, it is important to archive the new state of the device and the execution history to document the transitions after the initial production and deployment.

B. Architecture

Figure 1 illustrates the evidence collection process itself. The concept consists of four main processes - measurement, editing, transmission and archiving. The edit process is where the functions of the TPM take effect and the measured data is secured. The measurement and the editing occur as part of the operation of the Measurement Instrument. The archiving process, on the other hand, occurs as part of the Archiving and Evaluation Unit. The transmission process serves as the communication between these two units.

The MI uses one or more sensors which create MVs. The creation of MVs is called measurement. These sensors can either be inserted in the MI or be situated outside the system as stand alone devices. Here, it is not specified which kind of sensors are present. For now, it is assumed that all MVs are generated and transmitted correctly at any time. Thus, no further considerations are taken to protect integrity and authenticity of the data at this point. The MVs are input values for the editing process. The main purpose is to make sure the MVs conform to all legal requirements. The processed MVs are then transmitted to an Archiving and Evaluation Unit. At this point, it is optional to provide encryption to realise confidentiality with the transmission of data or not. In addition to signing the evidence records, the TPM is also used for remote attestation to prove the authenticity of the device to the AEU. Hence, the AEU can be sure to communicate with a trusted system. The AEU is in charge of the permanent storage of the processed Measurement Values and the final evaluation – the archiving process. Moreover, it provides the Measurement Instrument with system updates. In our system architecture, the AEU is found outside the MI as self-contained unit. However, since the whole procedure cannot be taken apart, the functions of the AEU could also be located inside the measuring device. Nevertheless, we define in our system architecture two units – the MI and the AEU. This is done for space reasons. Since, especially traffic measurement devices should not be bulky or conspicuous. The storage capacity of such devices will be limited (for economic reasons). Furthermore, these devices are often in locations difficult to access i.e. above motorways. It is not convenient to have the measurements stored in these places since they must be retrieved periodically. Consequently, data storage is sourced out and the measurements must be transmitted to the remote AEU. The AEU must provide enough storage capacity to permanently store all produced data. Additionally, if the evaluation of the system status information would be done on the MI itself then the component responsible for the evaluation must also be trusted. If the integrity of the MI is compromised it is likely that the evaluation part is also compromised.

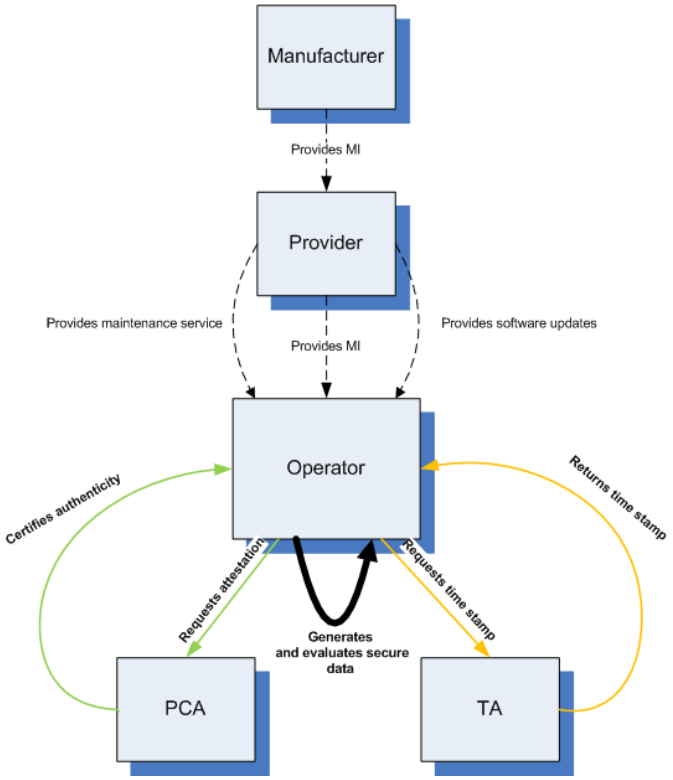

Fig. 2. Identified roles in the measurement protection process and their interactions

Logically, this is not acceptable for the design of a trusted system. Therefore, the evaluation of the measurement data and the system configuration is located outside the MI.

In summary, the architecture of the system consists of two main components – the MI and the AEU. Both components are responsible for compilation of processes that later result in a valuable legal outcome. The MI embeds the measurement sensors and the TPM and produces the actual evidence records. The AEU is responsible for storage capacity and high performance evaluation.

C. Extended roles

In this section the different relevant roles in the process and architecture described above are presented in mote detail. Figure 2 depicts the interactions of the roles.

The **manufacturer** as the producer of the MI generates the Endorsement Key and issus an Endorsement Key Credential for the TPM and a manufacturer certificate for the device itself. Through the issued certificates the manufacturer provides assurance that the EK was properly created and embedded in a valid TPM and that the device equipped with the particular TPM is in accordance to all specified requirements.

The **provider** can subsume different roles in the process. In the picture above, the provider is mainly responsible for the provision of the bundle of hardware platform with TPM, application software and reference Measurement Values for the software and for secure configurations. It may also be his responsibility to provide a possibility for archiving and evaluation (respectively, the AEU). This is optional to the operator. If the operator owns qualitative hardware and software resources then he might not need the provider to operate an AEU. Assembling the system, offering software updates as well as providing maintenance and repair services might be further responsibilities of the provider.

The **operator** possesses and controls the MI. His responsibility is operating the whole system and evaluating its outcome. This is to unify the tasks of the traffic MI and the AEU to form the main tasks of this role. To keep track of the different tasks of the different units they are described separately in the following paragraph.

The traffic MI collects data with its sensors which then is sent to the TPM for further processing. The TPM provides the hardware security for the MI. At this point, the MI further processes the MVs so that they meet the security requirements. Editing is done with the help of the TPM. The TPM provides certain means for the creation and secure storage of keys, for signing and time stamping data and for a secure data transmission to the AEU. Summarized, the MI must provide non-repudiation. The tasks of the AEU comprise the permanent storage of the MRs and their valuation. Since the MI usually does not have a graphical user interface, the AEU provides functionalities for displaying the collected data. Furthermore, the AEU is the interface to remotely update the software of the MI. Before any communication can occur, the AEU checks the system state of the MI. If the AEU is not communicating with the correctly identified device in a predefined system state the device is not used and maintenance processes need to be initiated. Detached from these entities, the operator himself is responsible to retrieve and prepare the evidence data e.g. for evaluation results in court.

As described in Section IV, out of privacy reasons a **privacy certification authority (PCA)** provides functionalities to supply privacy to the measurement data on the one hand and traceability on the other. The PCA provides attesting functionalities. Basically, this comprises the issuing of digital certificates. The PCA in issuing certificates attests that a public key contained in a certificate belongs to the entity noted in the certificate. Certificates in a TPM incorporate the attestation that a TPM was generated compliant to the standards and that a key was created correctly by the TPM. In our context, the PCA functionality is required to issue the credentials stating the origin of the data and binding the data to a particular MI. Another party puts trust in the PCA and verifies the PCA's signature to establish trust in a MI. The PCA is the so-called trusted third party (TTP). In our case, the TTP is in particular the AEU or the timing authority. It is possible that the manufacturer or the provider incorporate this role and issue certificates themselves. Always provided that, the certification takes place in a trusted and protected environment. Compromise of the CA leads to loss of security of the entire system.

The **timing authority (TA)** offers an adequate time stamping service such that a time stamp can be obtained that is

in conformity with legal regulations. A current time value is provided to the TPM which then will be synchronized with the current tick value of the TPM. So, the actual time of an event can be determined from a tick-stamp (a signature by the TPM including the tick value) and the initial timestamp of the TA. The synchronisation process needs to be repeated after each reboot of the TPM.

VI. Implementation

The following paragraphs discuss in more detail some of the previously mentioned solutions for the conception of a secure Traffic Monitoring Systems producing admissible evidence for legal proceedings. All presented solutions are build upon the security functionalities a TPM provides. In Section VI-0a a detailed description of a static and dynamic trusted boot process is given. Section VI-0b illustrates how additional security information is collected and added to the current Measurement Values forming a Measurement Record. The Measurement Record shall provide all necessary information for the admissibility of the produced Measurement Values e.g at court. The contents of a Measurement Record, the acquisition of the required security information and the signing operation on the Measurement Record are described. In Section VI-0c the acquisition of a real time value is presented. This value combined with an internal TPM time stamp is used to determine the exact time of the MV generation. Section VI-0d briefly describes the background of the transmission process.

a) Trusted Boot: Trusted boot offers the possibility to provide a basis for the trusted measurement of data. It is used to create a foundation for a trusted environment. With this kind of integrity check at the beginning of each boot process, it is trustworthy reported if a correct or a malicious or faulty system was booted. After the integrity check of the start-up phase the running systems integrity needs to be measured. Since the measuring device will be used for e.g. traffic analysis it is likely to be located outside in the field. As a permanently used MI it will not be under continuous personal surveillance. Attackers can get physical access. On the other hand, MI can be located above frequented roads out of physical reach. This could pose difficulties for some attackers to physically insert malicious code or manipulate hardware. However, more critical is the scenario where attackers use the communication interfaces to remotely insert malicious code. To prevent this, the executed applications must be checked for integrity via a dynamic extension of the chain of trust. The TPM continuously stores measured integrity values so that they can later be attached as additional information to the Measurement Record.

b) Measurement Records: From a legal perspective, with any mechanism implemented, the operator of a measuring instrument must ensure that data must be admissible if used as evidence in a court of law. Since the evidential integrity of digital data must be ensured the collected data must be secured against tampering. Usually this is done with so-called measurement logs or digitally signed records that save details about the measuring. A measurement log must contain different values like the device identification, initial function checks, regularly function checks, initial and end measurements, the name of the person carrying out the measurement, and the current time. To mention some possible requirements for measurement logs, [20] defines for radar equipment that the log must contain date and time of the measurement, the measured speed and the vehicle's direction of travel. If using a camera the log must enclose the correct association between the direction of radiation and that of the optical axis of the camera. Moreover, all device checks must be included in the log. [23] describes that in each picture or sequence of pictures the date and the time in a minimal resolution of seconds must be superimposed. The traffic situation must be documented so that no faulty association occurs. [23] depicts a variety of documentation methods and its requirements as well as the requirements on the device in general. What exactly is needed is subject to the local legislation and the actual purpose of the device.

Considering newer documentation techniques such as digital images, forgery and manipulation is obviously easier. Thus, additional mechanisms are necessary to provide for authenticity. Transport for London [27] said in their report that the evidential integrity of digital pictures must be provided (although only symmetric keys are used). Cottingham, Beresford, and Harle [7] noted that if digital images are taken they require digital signatures at the point they are taken.

As explained above, digital signatures alone do not provide adequate protection if the status of the device at time of measurement and signature is not known. To accomplish this additional protection another processing step is added to the creation of measurement data. This process based on our security assumptions adds additional evidence to the Measurement Values created by the system to log. The created documentation structure containing the raw values of the measurements plus additional information is called Measurement Record. The generic contents of a MR are:

Identity of the device Each device shall have a unique identity that is included in each measurement record. The TPM can provide such unique identities. Only data measured by a trusted MI is accepted. Further, a unique identification number is also associated with each Measurement Record.

Location Location information is required to prove that the MI was used at the correct position. Especially, for speed cameras restrictions on the positioning of the device are present. For example, it is important to set up the MI so that both sides of the road can be seen in the pictures and that the driving direction can be determined. For this, it is best practice to create a reference measurement when the device is installed and repeat them in periodical time intervals [20]. The location can implicitly or explicitly be given.

Measurement Values Raw Measurement Values are the data measured by the MI. MVs can be data in any format whether it is a speed representation, a number, a picture or a video. The MVs are the actual evidence that is used to prove that a particular event happened. Depending on the local legislation, MVs must be individually secured (signed, time-stamped, and encrypted) or can be secured in a set. Securing more than

one MV at a time would drastically increase the performance of the MI. The signature over the hash value of the MR guarantees that the hashed data originates from the MI holding the private part of the signing key. Thus, hash value and the signature ensure that integrity and authenticity of the MVs can be validated by the AEU. Consequently, the actual data of the MVs can be transmitted to the AEU separately from the digital signature. Corruption of the MVs can be determined through the hash value and the signature enclosed in the MR.

Time The time stamp is specifically added to each MVs at the time of their creation. The time stamp is needed for proving the time of the happened event. The v1.2 TPM specification newly defines a Tick Counter [28]. The time stamp created by the TPM is no real time value but a tick initialised to a particular vale and counting in fixed time steps. Thus, the tick count of the TPM needs to be associated to real time information from a reliable and trusted time authority. This association shall be repeated in regular intervals to ensure that tick count and real time remain synchronized.

System Status The system status must be documented to provide the MVs with a proof that the system was running correctly and no faults occurred during the creation. This can be done either explicity by adding the result of a TPM_Quote to the MV or implicitly, by using a sealed key to sign the MV.

c) Time Stamping: As described in the previous sections a time stamp is added to the measurement data. The utilized time stamp actually is a timing value associated with a signature. A time stamp is used out of two reasons. First, with time stamps the point of time an event happened is assured. Second, it must be proven that the measured data has not been altered since it was seized. With the combination of time stamps and signatures one distinct moment can be determined when data was known to be correct and unaltered. In particular, when initiating legal action, it is necessary to prove the integrity of measurement data many years after the evidence was assembled. Time stamps can bind the measured data needed to secure, the device identity and the time of an event. Once bound, the integrity of data can be determined years after the data actually was collected. It just needs to be warranted that the utilized time stamps are tamper resistant and auditable. Hosmer said that secure and auditable time stamps improve the integrity of digital evidence as well as they provide higher assurance required for the digital chain of custody. Later, Hosmer defined attributes for secure, auditable digital date/time stamps [6, p. 4].

d) Transmission: As the last step the transmission of the Measurement Records needs to be secured. It is necessary to establish a secure connection in between the communication partners, i.e.. the AEU and the MI. First, the authentication of the AEU towards the MI must be ascertained. Authenticating the AEU is essential to securely transport the Measurement Records to the right destination (the AEU) or to be ensured that updates are received from the right source. Second, the AEU shall be ensured that it is communicating with a trusted MI and that this MI is in a trusted system state. And third, the transmitted MRs shall be secured against spoofing or other attacks. No attacker shall be able to change, read or obtain information contained in the MRs.

To assure that the AEU communicats with the right MI a Trusted Computing concept is applied. The paradigm of remote attestation in conjunction with a privacy CA can be used to assure the correct operation of the MI. This concept allows for authentication towards a third party and, at the same time, for approval of the integrity of the system. The TPM uses a certified key pair (AIK), that classifies the platform as a genuine TCG platform, to sign the current PCR values. Similar approaches can be found also in [11], [13]. Depending on the system design, the AIK could be created during the manufacturing process and be equipped with an AIK credential. In this case, the manufacturer or provider would adopt the role of the PCA to certify the trustworthiness of the AIK. Or the AIK is created at a later stage and the certificate is remotely issued by a PCA or another trusted entity. Before delivering of measurement data can take place the AEU has to challenge a MI to attest its current configuration. The MI sends the signed PCRs together with the measurement log containing each of the individual measurements that have been added to the PCR hash chains. Also, the certificate attesting the trustworthiness of the AIK is sent. The AEU reviews both to verify the correctness of the certificate and system state. If the verification turns out to be positive the Measurement Records can be transferred and regarded as trustworthy.

VII. Conclusions

Non-repudiation for processes without physical evidence is more and more important for practical use cases due to the increase of IT based systems and IT supported processes. This paper presented a first step towards the development of Measurement Instruments used for the collection of evidence with increased probative force. The design of a trustworthy evidence collector implemented by applying concepts from the Trusted Computing domain is hereby the main contribution. Through the introduction of hardware based identities and the concept of authentication of behaviour a new level of reliability in the collected evidence with respect to the non-repudiation can be reached. Furthermore, in the analysis of the processes around such a solution shows that for reliable digital evidence organisational processes as well as the state and environment of computational devices are relevant. The design of the MIs shows that the forensic use of digital data can and should be considered already during system engineering. Fundamental design decisions early in the design process are needed to achieve a high level of reliability and security of forensic data.

Further research in this domain will lead the authors to (i) a technology oriented development of embedded hardware trust anchors for an extended support of this special use case and (ii) research towards the application in real world scenarios considering legal and organisational aspects.

References

[1] J.P. Anderson et al. Computer Security Technology Planning Study., 1972.

[2] P.T. Blythe. Congestion charging: challenges to meet the UK policy objectives. *Review of Network Economics*, 3(4):356–370, 2004.

[3] Matthew Braid. Collecting Electronic Evidence After a System Compromise, 2001.

[4] M. Bramberger, R.P. Pflugfelder, A. Maier, B. Rinner, B. Strobl, and H. Schwabach. A smart camera for traffic surveillance. In *Proceedings of the First Workshop on Intelligent Solutions in Embedded Systems*, pages 153–164. Citeseer, 2003.

[5] E. Brickell, J. Camenisch, and L. Chen. Direct anonymous attestation. In *Proceedings of the 11th ACM conference on Computer and communications security*, pages 132–145. ACM New York, NY, USA, 2004.

[6] Inc. Chet Hosmer, President & CEO WetStone Technologies. Proving the Integrity of Digital Evidence with Time. *International Journal of Digital Evidence*, 1(1), 2002.

[7] David N. Cottingham, Alastair R. Beresford, and Robert K. Harle. A Survey of Technologies for the Implementation of National-Scale Road User Charging. *Transport Reviews, Volume 27 Issue 4*, July 2007.

[8] D. Eastlake and P. Jones. US secure hash algorithm 1 (SHA1), 2002.

[9] Michael Kasper, Nicolai Kuntze, and Andreas U. Schmidt. On the deployment of mobile trusted modules. In *Proceedings of the Wireless Communications and Networking Conference WCNC 2008, Las Vegas, USA, 31 March - 2 April 2008*. IEEE Press, 2008.

[10] R. Kühne. Die Straßenmaut in Deutschland-Richtlinienkonformität und Vereinbarkeit in Deutschland. 2003.

[11] Nicolai Kuntze, Andreas Fuchs, and Carsten Rudolph. Reliable Identities using off-the-shelf hardware security in MANETs. In *Proceedings of the International Symposium on Trusted Computing and Communications (TrustCom 2009)*, 2009.

[12] Nicolai Kuntze, Dominique Mähler, and Andreas U. Schmidt. Employing trusted computing for the forward pricing of pseudonyms in reputation systems. In *Axmedis 2006, Proceedings of the 2nd International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution, Volume for Workshops, Industrial, and Application Sessions*, 2006.

[13] A. Leicher, N. Kuntze, and A.U. Schmidt. Implementation of a Trusted Ticket System. In *Emerging Challenges for Security, Privacy and Trust: 24th Ifip Tc 11 International Information Security Conference, SEC 2009, Pafos, Cyprus, May 18-20, 2009, Proceedings*, page 152. Springer, 2009.

[14] Michael LeMay, George Gross, Carl A. Gunter, and Sanjam Garg. Unified architecture for large-scale attested metering. In *Hawaii International Conference on System Sciences*, Big Island, Hawaii, January 2007. IEEE.

[15] Michael LeMay and Carl A. Gunter. Cumulative attestation kernels for embedded systems. In Michael Backes and Peng Ning, editors, *ESORICS*, volume 5789 of *Lecture Notes in Computer Science*, pages 655–670. Springer, 2009.

[16] Stephen Mason, Philip N Argy, Ruth Cannon, Stephen Coughlan, Robert J Currie, Brian W Esler, Lorna Goodwin, Julien Hofman, Manisha T Karia, Tejas D Karia, David Leung, Iain G Mitchell, Laura O'Gorman, Damian Schofieldand Daniel Seng, , and Bryan Tan. Electronic Evidence: Disclosure, Discovery and Admissibility. *International Commentary on Evidence*, 2007.

[17] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone. *Handbook of applied cryptography*. CRC, 1996.

[18] C. Mitchell et al. Trusted Computing. *Trusted computing*, page 1, 2005.

[19] Richard Nolan, Colin O'Sullivan, Jake Branson, and Cal Waits. First Responders Guide to Computer Forensics, March 2005.

[20] OIML International Organization of Legal Metrology. Radar equipment for the measurement of the speed of vehicles. OIML R 91, 1990.

[21] John Patzakis. Maintaining The Digital Chain of Custody, April 2003.

[22] S. Pearson. Trusted computing platforms, the next security solution. *HP Labs*, 2002.

[23] Physikalisch-Technischen Bundesanstalt (PTB). PTB-Anforderungen - Messgeräte im Straßenverkehr Geschwindigkeitsüberwachungsgeräte. PTB-A 18.11, November 2006.

[24] D. Piester, A. Bauch, J. Becker, and T. Polewka. Time and frequency activities at the Physikalisch-Technische Bundesanstalt, 2004.

[25] Geoffrey Schmitt. Acting as an Expert Witness, 2007.

[26] Sergio L. Toral, Manuel Vargas, and Federico Barrero. Embedded multimedia processors for road-traffic parameter estimation. *Computer*, 42:61–68, 2009.

[27] Transport for London. London Congestion Charging Technology Trials Stage 1 Report Version 1.0, February 2005.

[28] Trusted Computing Group. TPM v1.2 Specification Changes, October 2003.

[29] Trusted Computing Group. TPM Specification Version 1.2 Revision 103. *Trusted Computing Group*, 2009.