**Abstract**

We describe a concept to employ Trusted Computing technology to secure Conditional Access Systems (CAS) for DVB. Central is the embedding of a trust anchor, e.g., a trusted platform module (TPM) into the set-top box or Conditional Access Module. Various deployment scenarios exhibit possibilities of charging co-operation with mobile network operators (MNO) via trusted mobile devices, or with other payment providers.

**Keywords**

Trusted computing, conditional access system, content distribution, payment and charging.

**I. INTRODUCTION**

Delivery of digital content to customers is an emerging market with high potential revenues. For various business cases protection of the consumption good as a base for charging processes is required. Digital Video Broadcast (DVB), as the widest spread standard for digital content delivery, comprises methods for the protection of media data. DVB exists in diverse branches for special for different broadcasting techniques and formats: Satellite (DVB-S), cable (DVB-C), terrestrial (DVB-T), and mobile environment (DVB-H). The signal is encrypted with the Common-Scrambling-Algorithm (CSA) using an 8 byte seed for initialization, the so called Code Word (CW). This Code Word is provided by the Conditional Access System (CAS) [12, 1]. There are many vendors like Cryptoworks or NDS offering CAS Modules to content providers, see Table 7.1 in [Eimear-IEE]. The CAS has the essential task to bridge between the encrypted data stream and a smart card providing CWs. Due to various different CAS systems the customer needs different smart cards, often for exclusive use with different, proprietary Conditional Access Modules (CAM). CSA was kept as a secret over a couple of years, but was revealed some time ago [1]. Until now CSA is not broken.

Charging and payment is another purpose of the smart card – set-top box (STB) combination, a market which is dominated by smart card subscriptions. The customer registers the card after purchase with the provider and is able to descramble the digital stream for a certain time. On this basis, pay per view schemes, e.g., for single movies, can be realized. Actual charging is sometimes solved by using value added telephone services. A second way of charging for DVB content is using mobile payment solutions. One (German) peculiarity is the use of debit or credit cards in combination with a feedback channel of the set-top box [2].

The traditional DVB architectures have some common problems associated with the stand-alone nature of the set-top box, the unavailability, respectively, costliness of an upstream channel, and the smart card-based security architecture:

1. The update of decryption algorithms and secret keys and generally the remote management of the STB, e.g., subscriber management and channel bouquet selection, are difficult and costly.
2. Accounting and charging is generally realized as an out-of-band process more or less tightly linked to smart card roll out. On-line charging solutions are scarce and of provisional nature.
3. Users selecting bouquets from a variety of subscribers have to handle a number (ever increasing as the market diversifies) of smart cards manually.
4. If bouquet selection is done via the DVB down link, sending of personalized data for this kind of access control over the DVB channel is costly and does not scale well for many subscribers.

The focus of this paper is to provide practical improvement of the existing content protection schemes used by the DVB standard providing benefits in terms of customer satisfaction and price of the individual device. Other work in this area is focused in a more general security analysis as by Gallery [1] and Mitchell [4]. These security-theoretic approaches may be integrated in the scenarios discussed in this paper. Nevertheless, from a economic perspective the relevance of certain protection targets like freshness and proof of origin has to be examined with respect to the practical importance.

We propose architectural concepts based on Trusted Computing (TC), to improve on this state of the matter, and present a high-level design of a trusted set-top box (STB) which can be reconfigured for
various content protection schemes and payment methods. At the core of the concept lies a trust-enhanced CAM in Section III.A. In particular it realizes descrambling methods in software while protecting the associated access secrets of each provider. This usage of TC for STBs is rather traditional and feasible with minimal architectural changes. In a further step, we assume in Section III.B that the trusted STB has some sort of access to a communication network and use the latter for take ownership of it, i.e., the process of impressing a user identity and associated credential to the STB. This essentially obliterates the use of smart cards. Finally we discuss options for integration of charging functionality using a mobile device communicating with the STB in Section III.C, and discuss concrete payment scenarios in Section III.D. The main benefits of deployment and usage of trusted STBs and advanced utilization options are discussed in Section IV. Section V. concludes the paper and an Appendix compiles essential details about Trusted Computing used in the main text.

II. TRUSTED COMPUTING
The idea of building security into open, connected systems by using TC-enabled platforms has a long history [3, 4, 5]. These platforms are characterized by a few key properties.

A hardware security anchor is the key to the protection of the system behaviour and acts as a root of trust for its secure operation. Secondly, functional building blocks in a system that are assumed to be trusted, i.e., to behave in a well-defined manner for the intended purpose, form the Trusted Computing Base (TCB) of the system. The TCB comprises such components of a system which cannot be examined for trustworthiness during operation, but only by out-of-band processes like compliance and conformance testing, validation, and certification.

The TCB together with the hardware security anchor can be used to turn a system into a trusted platform (TP), which is a very ambitious, and still today theoretical, concept. The key concept is the extension of trust in an open system from the root to other, loaded or otherwise changing components using the TCB’s capabilities. This extends the trust boundary of a TP beyond the root and the TCB, and is commonly realized by cryptographic mechanisms of which both are capable. The establishment of the trust boundary is conceptually associated to the boot cycle of the platform. Certain functions of the hardware root and the TCB are started before other parts of the system and operate as a root of trust for measurement. This means that components that are started or loaded later on, are measured, i.e., digest values over a component’s software parts, parameters and loaded programs are generated and stored protected by the root of trust. This process, if executed up to the OS loader and OS, is called authenticated boot.

Yet more involved is the concept of secure boot. It is of particular importance for devices like set-top boxes or mobile handsets that necessarily have some stand-alone and offline functional requirements. In secure boot, the device is equipped with a local verifier and enforcer supervising the boot process. They compare measurement values of new components with reference values (in a protected storage space) and decide whether they are loaded or not. Thus the system is ensured to boot into a pre-defined, secure state.

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 verifiably 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.

Today, TC is mostly associated with the standardization efforts of the Trusted Computing Group [6, 7], on which also our proposed concepts build. An overview can be found in the Appendix.

III. CONCEPTS AND DEPLOYMENT SCENARIOS
Trusted Computing technology can be useful at several stages in the lifecycle of digital broadcast content [8]. Here we focus on the user terminal and questions of controlled access to content and present three concrete scenarios for TC application, in order of increasing complexity.
A. Trust-enhanced CAM

Based on the basic features of TC a soft realization (or even virtualization) of the CAS is feasible. Implementing in this way a trusted set-top box in the context of DVB can be done in many variations. An elementary implementation stores the functionality of the CAM as software protected by means of the TPM. If the user requests a scrambled channel, the set top box uses the CAM software to create the respective code words required by the CAS. A proposal for pertinent system architecture is shown in Figure 1. Starting with the smart card on the right hand side, we observe a main conceptual change w.r.t. traditional CAS: The smart card bears merely the subscriber identity and credential. All other security-critical functionality is shifted into the trust boundary of a trust-enhanced CAM and protected by a hardware security anchor, e.g., a TPM. The TCB enables and protects upper functionality of the CAM via a secure boot process. The protected CAM functionality comprises three essentials: i) A management software and protected, non-volatile storage for access secrets used by the single CW generators. ii) An interface to the smart card providing a secure channel to import user credentials. iii) A secure interface to import new algorithms and access secrets.

The access credential manager invokes soft instances of Code Word generators on demand, using the required access secret, e.g., Control Word (CW). Security of the CAS realized in this way relies on the fact that CW generation is within the trust boundary, i.e., the system state of the CW generator and access secret manager is trustworthy and tamper-resistant. The TCB of each Set-top box is equipped with a credential which identifies it as belonging to some group or individually. This enables end-to-end (e2e) encrypted communication from the provider’s headend [9] to the Trust-enhanced CAM. This credential can be impressed at an early stage of the STB’s lifecycle, e.g., by the manufacturer, the OEM, or a service provider. It can be located in the hardware trust anchor or be protected by it. New access secrets and usage policies can be transferred to the CAM in the common Entitlement Control Messages (ECMs), Entitlement Management Messages (EMM) respectively [9], distilled from DVB stream [11, 12, 13]. They are, in our scheme, e2e-encrypted for the particular CAM and enable the management software to fell authorization decisions. Comparing the subscriber identity with the policies for e.g., bouquet access in the EMMs, the manager will decide whether to import the associated Control Words which embody the access secrets for the bouquet. Algorithms can be updated for each CW generator, for instance via IP-over-DVB [14].

Some key advantages of a trust-enhanced CAM are obvious. It resolves the focal problems 1. and 2. described above. The CW generators can be realized in software and implement a variety of different CW generation algorithms. These algorithms can be updated “over the air”. Additionally it has the technical advantage that the frequent sending of ECMs for security reasons becomes obsolete, since the derived access control secrets, commonly today the Code Words used for initialization of the CSA, are managed inside the trust boundary and hence are not easily accessible to attackers. This helps to address problem 4.

The trust-enhanced CAM enables a modular system where it is possible to replace every part of the descrambling in a trustworthy way. Using for instance Field Programmable Gate Arrays (FPGA) technology on top of TCB and root of trust enables the replacement of every part of the existing DVB architecture. This makes it possible to implement algorithms in hardware to gain speed. FPGAs are programmed (reconfigured) before they can perform the desired task. Trustworthy implementations can verify the content of the FPGA before data are transmitted between FPGA and the CAM.

In a more evolved scenario the root of trust, e.g., TPM, could be an integral element of the code word scheme replacing the smartcard.

B. Online CAS

A system which emulates the actual CAS systems in software has to enforce that keys used to generate the CWs required by the CAS are kept secret. The security of the proposed system has to be guaranteed even if the algorithm is published. Beside this technical requirement online verification of the access rights as a second requirement is the premise for dynamically granted content access. This leads to an authentication scheme where the CAS asks for permission before the CWs are created. Therefore a connection is established by a communication module granting access to a network.
A protocol solving this problem has to perform the following steps. In preparation an appropriate roll out of the set-top boxes has to happen. During the roll-out a take ownership by the provider is required. A network operator can be used instead of the provider assigning user identities and, optionally, performing charging processes. The proposed scenario consists of four parties: customer, provider, charging provider, and network operator as depicted in Figure 2. The network operator issues the set-top boxes to the customers in the same way as they offer mobile devices. The bonding between customer and device is based e.g. on a SIM-card. An online take ownership is as well possible as described in the subsequent section.

The network operator establishes his trust in the device by a network operator issued credential which is produced by the box on request. Based on this underlying trust relation the (M)NO can assure the identity of the set-top box to a supplier. This second (transitive) relation [15] is based on a second credential issued either by the network operator or the trusted set-top box. In either case the network operator in his role as an identity provider (ID) signs this credential which therefore is stored in the trusted set-top box. If a customer decides to consume a certain service it offers this credential to the vendor (V), for instance the content provider. V uses this credential to verify the identity against ID. V then delivers the content and requests charging by ID. In this scenario the user is unknown to V as the credential is only validated by ID. ID does not need to reveal the user identity to V.

Delivery in this context means that V transfers a secret into the trusted set-top box and adds this secret to the list of accepted credentials as this is known by the actual process of conventional CASs. This secret is sealed in the set-top box by using the sealing functionality of the TPM. This means the issued secret can only be used in the same trustworthy state of the box. The root of trust in this case is the ability of attestation of the integrity to a third party e.g. V or ID. An advantage is that personalized data e.g. for bouquet access needs not to be transferred via the costly satellite downlink.

In an online CAS a tight interweaving between content access control and payment scenarios is possible. This is discussed in the following section.

C. Online take ownership / online registration

The aim of an online take ownership procedure is to establish a user identifying credential into a trusted set-top box without the need to issue the box over a special infrastructure provided by ID. The customer should be able to buy such a box everywhere she wants. During production every box gets an identifier in form of the unique platform certificate. Based on this initial credential a protocol can be performed to establish a user related certificate. This user certificate is used to identify the user at V. The used protocol establishing this user credential depends if there is a direct or indirect communication between V and ID.

The user certificate can be created after the take ownership process of a trusted platform which binds a TPM to a certain user using a 160 bit authentication value (TPM owner authorization). AIKs are available after the take ownership to be used as credentials testifying the identity of a user. An AIK can only be created offering a valid TPM owner authorization and is a private/public key pair. The private portion is shielded inside the TPM. After this, a privacy CA issues a certificate to assert the relation between AIK and TPM (see the Appendix). For this initial AIK and certificate creation process an online connection to a privacy CA is required. The pertinent protocol has to protect the origin of the key so that it is impossible to fake a TPM.

In the case of a direct communication the system is equipped with a communication device enabling the direct contact to the privacy CA. In this case the mentioned protocols can be used without any restrictions. If the system is not equipped with such a communication device at least a short range communication is required enabling a take ownership over a secondary communication device (SD) like a cell phone. The SD forwards the communication in the respective direction. The ensuing set of communication relationships is shown in Figure 3.
It is important to mention that there has to be a trust relation between the privacy CA and the content providers. In this use case AIKs are used as tickets which enable accounting. Therefore it could be possible that the privacy CA should be able to reveal the identity of a certain AIK, e.g. in case of suspected fraud.

After the take ownership an online registration at the respective provider is required to sign up to a certain service. In this process two goals have to be achieved. First, the identity of the mobile device (and therefore the identity of the user) has to be registered at the service provider. By issuing the AIK and the belonging certificate the identity can be proved and by performing a handshake protocol between service provider and mobile device the origin is testified. The second aim is to negotiate about the details of the subscription. One part of these details is the payment information. The service provider transmits a data structure which describes the available charging models and services. The user selects from this offer, signs the selection with the private portion of the AIK and transmits this to the service provider.

A proof of authenticity of the service provider is also required. Hence it is necessary to sign messages issued by the service provider. A verification of the authenticity can be achieved using known PKI structures or built-in root certificates. Alternatively, the MNO can vouch for the authenticity of a certain service provider replacing conventional PKI systems.

Figure 4 shows a basic scheme using AIKs as authentication tokens. The protocol is divided in two phases. Phase 1 is concerned with AIK creation and certification, phase 2 is the usage of this token. The set-top box transmits in 1) certain credentials of the platform and the public portion of the AIK to the PCA which verifies the offered credentials and then retransmits (2) a certificate stating that this AIK belongs to an accepted platform. If the MNO works as PCA the AIK can later be used as a payment credential as the MNO can reveal the identity of the users based on the certificate. This feature is used in phase 2 where the set-top box offers the AIK and the corresponding certificate to a service provider (3). This service provider performs an attestation of the box in this step and then request from the CA the validity of the offered certificate (4,5). 4 and 5 can be performed e.g. using OCSP responder known from PKI infrastructures. Step 6 returns the acceptance information of the service provider (this answer should be signed by him). To validate the signature on side of the set-top box an appropriate certificate must be available in the device. It can be necessary to request this root certificate from a trustworthy third party. After this the set-top box has been successfully registered at a certain service provider.

Let us discuss algorithm updates mediated by the mobile device in some more detail. As stated in the introduction the scrambling of the digital content relies on the security of the CSA. This algorithm has to fulfil two requirements. The first is to provide a secure scrambling of the data. The second is the real-time environment. The digital stream has to be descrambled in the moment it arrives. This leads to a lack of algorithm strength and the need to replace the algorithm can be foreseen [16, 17], entailing a complete change of the installed infrastructure on side of the customers as well – a very costly and inconvenient effort.

From the viewpoint of customer satisfaction it is advantageous if it is possible to update a certain device to new required standards and protocols. As introduced in the online CAS section, it is possible to implement the complete CAS as a software module protected by the underlying TC architecture. Depending on the implementation, modules of the
DVB system can be updated by a software protocol. The update process can be started by the system based on an explicit user request. First, the device transmits a nonce and a device description data block (DDDB) to the update service which is signed by the AIK. Depending on the DDDB the update service creates a data block containing the new firmware of the device and signs it with the signing key of the update service. This data is then encrypted with the AIK and send to the device. The device then decrypts and checks the received data and updates the system. If reprogrammable hardware such as FPGAs the update results in a reprogramming of the hardware. It is important to consider reliable checks of the content of such hardware and hardware based methods which are protecting the content of such hardware against fraud.

D. Payment Scenarios

Trusted computing offers the possibility for client-side payment systems. The main idea is that the set-top box handles charging in equivalent to prepaid or pay-as-you-go scenarios. The box meters the consumption of the digital content. Either an internal deposit is decremented or the consumption data is stored and after a certain time read by V and charged. The second alternative requires a trusted time source in the device to enable time stamps for the recorded metering data. This time source can be implemented as an online time authority which offers a timestamping service. Another option is an internal time source based on the trusted platform. This shall be discussed elsewhere. A third usage scenario is the well known distribution of keys which are descrambling a channel for a certain time. The first alternative requires a central authority to increment the internal deposit. Therefore it is required to transmit the increment value to the respective box. The increment value is signed by the concerned charging service and encrypted by the public portion of the AIK. These two steps are ensuring that this packet is bound to one device. Preventing a replay attack requires the inclusion of: (i) attestation of the particular device by the charging service testifying the integrity of the device, and (ii) integration a Nonce issued by the charging service to prevent that the packet is used twice. The box stores these Nonces and rejects replayed packets. A basic protocol works as follows. In step (1) the box requests for an increment of the internal deposit, offering the AIK and a corresponding certificate. Step (2) performs an attestation and within this step a handshake testifying the correlation of the AIK and its certificate. At some point in these first two steps the charging provider has to decide if he accepts this AIK based on a contractual relation to the user or its charging provider and PCA. After step 2 the charging provider has to decide which amount is transferred to the box. This can be done based on a pre-paid scenario, a pay-as-you-go scheme, or other contractual scenarios like charging the telephone bill of the user if the PCA or the charging provider is operated by the MNO.

Storing the consumption in the device is the second alternative. Here it is possible to offer the user the possibility first to consume the content and afterwards to pay for it as it is known from e.g. cellular phones. The stored consumption data are transferred to the charging provider either by a push system where the box is in charge for transferring the data to the provider or by a pull system where the provider requests the data from every box. The most significant difference between these two schemes is the signalling of the box as the pull solution requires a built in communication device like a GSM module. Building on a push solution another device like a mobile phone can be utilized to transfer the data to the charging provider. Important to note in the second case is that the logged data require a special protection against forgery. Therefore each consumption log record needs to be time stamped by a trustworthy time source. After the transfer of the consumption log the charging provider charges the consumer belonging to the system. This relation between consumption data and user is expressed by signing the data with the respective AIK which was first registered at the charging provider (see last section). As a privacy protection after the signing the data can be encrypted by a public key belonging to the charging provider. By this an MNO or any third party listening to the data stream cannot create usage profiles of the customers.

A third alternative is based on usage credentials which are basically descrambling keys inserted e.g. in the conventional CAS implemented in DVB and enhanced by a constraint of e.g. its usage period. Other constraints are also possible. Examples are maximum boundaries of daily usage, or time of usage. Issuing such a restricted key to a system requires (i) an attestation of the system before the key is transmitted to proof the integrity of the system, (ii) a PKI structure to enable the system to verify the origin of the data, and (iii) a charging infrastructure which maintains the keys. Based on the CAS system it can be necessary to store the key in a sealed environment as it is offered by the TPM sealing functions. A variant of this kind of content protection is exhibited in [18].

IV. DISCUSSION AND ADVANCED FUNCTIONALITIES

A. Security and realizability

Security of the trust-enhanced CAM of Section III.A and the subsequent concepts hinges on the trust boundary of the platform established by a) the hardware security anchor, b) authenticated or secure boot, and c) security of the components of the TCB.
On the other hand, the security of the traditional system is on the well-established level of smartcards. The main difference, which holds for most protection concepts based on TC, is that security critical data like access credentials, in particular EMMs, are held and used in the ordinary storage of the platform. Though they are protected by encryption via the hardware root of trust, they are not protected by physical separation during operations with them, as is the case with, e.g., decryption keys which are only used on a smartcard and never leave it. To establish a similar protection level, the TCB must contain functionality to secure data in the memory and upon transmission to, e.g., the processor or other components. Such are known as secure channels and exist in several variants [19, 20, 21].

If it makes practical and economical sense to raise the security of a trust-enhanced CAM to that of smartcards depends on the `commercial grade security` required in a concrete business scenario. First, the CAM is still a separate module which allows for inexpensive physical protection against tampering. Second, the maximum damage incurred by providers if a credential (e.g. an EMM) is compromissed on a single platform is a new rollout of the latter. This does, however, not repair the potential for leakage of content through the compromised platform on which an attacker has found a way to obtain EMMs. This is a principal problem of the DVB architecture, which has led to costly replacements of hardware in the past. Trust-enhanced CAMs and STBs can be useful for a resolution of this problem, since their root of trust provides credentials to uniquely identify the platform, in particular in an attestation process. Thus it may be possible, using secondary communication channels like the mobile network, to disable a compromised platform and protect the DVB system as a whole.

We believe that CAMs and STBs are interesting for TC deployment and usage. Most STBs are restricted PC platforms running standard OS. For them, a lot of TC hard- and software is available. Thus our concepts seem to be realizable in the near future.

B. Benefits of TC for DVB systems

A trusted set-top box enables the creation of a universal decoder for broad range of different scrambling systems without the need for the user to physically change the smart card. The virtualization of the CAS hardware is also interesting for reducing the costs of a single set top box. This can sensibly be combined with either a long range communication module, e.g. GSM or UMTS, or a near range communication module like Bluetooth or NFC. This enhancement enables complex scenarios with respect to accounting and charging, some of which are presented in the following list.

- As mentioned, the communication between the trusted set-top box can be performed by an integrated long range communication device or a near range device. Using GSM/UMTS in a box enables the cooperation between a mobile network operator who can offer accounting, charging, and maintenance for the customers and box vendor/DVB provider. The MNO is also able to offer a well tested authentication system in form of the SIM-card known in the mobile domain. Based on this primary identifier other authentication schemes using the TPM are possible as they are introduced in [22].
- Online payment using e.g. credit cards in the set-top box is one of the most important possibilities which are enabled by trusted set top boxes.
- Implementing an online CAS Module which replaces the CAS-Smartcard complex can eliminate the possibility of using fake smart cards as the box can control the access rights by an access control list at the side of the provider. TC provides in this scenario the authenticity and identity of the box and the attestation of its integrity (by the TC methods of remote or direct anonymous attestation). With these basic assumptions it is possible to implement a trustworthy client side CAS.
- As the set-top box can be considered as trustworthy, such a box enables easy-to-use payment schemes which have the potential to replace existing Pay-per-View schemes. By executing charging on the client side, price schedules can depend on the consumed service or content which can be metered by the trustworthy box. It would as well be possible to recognize debit and credit cards or to prepay various contents.
- Online Algorithm updates for video decryption are an extension of the variants above, which enables on demand reconfiguration for unknown decryption schemes or the exchange of existing ones. The vendor or broadcaster can issue in a standardized configuration file the new algorithm which is to be used in the box to decrypt the incoming video stream. This also enables over the air enhancements and updates of the trusted set top box e.g. faster implementations.

Near range communication devices like Bluetooth require SDs like mobile phone as communication intermediaries to the broadcaster. As it may be cheaper than a dedicated GSM module in each set-top box this could be the better choice. This solution requires charging in the set-top box as described above. Charging and updates are performed by using SD. After this step the set-top box works autonomous.
C. Multi-CAS management
New accounting and charging systems can be established using the TPM and the trusted environment. Here the sealing functionality is highlighted, as a replacement (or new specification) for the CAS. One box can house various CAS concurrently without any extra hardware costs. Charging can be transferred into the Box by adding specialized software and appropriate hardware. The trustworthy state of both can be proved in the trusted boot process and attested to an external verifier by remote or anonymous attestation. The box can handle the charging process and control the access to the charged commodity. By this, new payment infrastructures can be established, e.g., for home shopping.

D. Mobile co-operation
The presented concepts offer a high degree of co-operation of DVB service providers with mobile networks and their MNOs. This co-operation brings major benefits, though the technology DVB is not common in the mobile domain. The MNO can provide primary services to DVB operators or broadcaster:

- Management of subscribers
- Potential merging of the subscriber bases
- Charging
- Dynamical control of security features
- Enhanced CAS security
- Marketing co-operation

Furthermore the concept can complement current or development mobile content protection like OMA. In effect it enables MNOs to enter a mobile video broadcasting partial market. The underlying concept is not limited to DVB. It can enhance or substitute existing CAS systems for streaming multimedia applications. It is also possible to combine this with a bonding of the set-top box to a special mobile phone or network operator. A network operator can offer set-top boxes as part of their customer retention.

E. Client-side watermarking
As an extension the box can apply certain digital rights management (DRM) functionalities upon the digital content. These restrictions can be applied by the box dependent on the contract between the partners. These restrictions can for example regulate the count of allowed copies. Depending on the rights purchased by the user different usages of the content (multiple viewing, multiple private copies, quality discrimination, commercial-free versions, etc) can be permitted by application of DRM techniques. As every customer can buy different rights for one digital asset this restriction have to be added on customer side. It could also be intended, as an alternative to 'hard' DRM, to tag a digital asset and by this to suppress the distribution. This leads to the need to include a marking identifying the individual customer, while still preserving his/her privacy. This service can be a major reason to apply watermarking at client-side. This can be implemented with ease within the trusted set-top box based on our concepts.

V. CONCLUSIONS
We have shown that turning set-top boxes and/or CAMs into trusted platforms according to TCG specifications offers attractive novel possibilities for DVB content distribution, CAS operation, and payment. Prerequisites for implementation seem rather low as today’s set-top boxes are already full-fledged PCs and TC will be ubiquitous in the near future.

APPENDIX

Trusted Computing Essentials
The Trusted Computing Group (TCG) is the main industrial effort to standardize TC technology. It currently enters the mobile domain [3] with the aim to provide a standardised security infrastructure. 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 (TPM), 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.

As it is currently being standardized in the PC and mobile domain offers a highly flexible and reliable security infrastructure enabling various kinds of authentication, authorization, and audit schemes. A TPM provides a unique identity of the particular device, and cryptographic abilities for creation, storage such as usage of asymmetric key pairs. On top of these TPM abilities, TC offers a metric to measure the system state and to report this measurement to a third entity. A further main ability is to bind certain data cryptographically to the particular platform and its state.

Through the TPM the TP gains a cryptographic engine and a protected storage. Each physical instantiation of a TPM has a unique identity by an Endorsement Key (EK) which is created at manufacture time. This key is used as a base for secure transactions as the Endorsement Key Credential (EKC) asserts that the holder of the private portion of the EK is a TPM conforming to the TCG specification. The EKC is issued as well at production time and the private part of the key pair does not leave the TPM. There are other credentials specified by the TCG which are stating the conformance of the TPM and the platform for instance the so called platform credential. Before a TPM can be used a take ownership procedure must be performed in which the usage of the TPM is bound to a certain user. The following technical details are taken from [6].
The TPM is equipped with a physical random number generator, and a key generation component which creates RSA key pairs. The key generator is designed as a protected capability, and the created private keys are kept in a shielded capability (a protected storage space inside the TPM). The shielded capabilities protect internal data structures by controlling their use. Three of them are essential for applications.

First, key creation and management, second the ability to create a trust measurement which can be used to assert a certain state toward a remote party, and finally sealing methods to protect arbitrary data by binding it (in TCG nomenclature) to TP states and TPM keys.

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 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 involved 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 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. The protocol for issuing this credential consists in three basic steps. First, the TPM generates an RSA key pair by performing the TPM_MakeIdentity command. The resulting public key together with certain credentials identifying the platform is then transferred to the PCA. Second, the PCA verifies the correctness of the produced credentials and the AIK signature. If they are valid the PCA creates the AIK credential which contains an identity label, the AIK public key, and information about the TPM and the platform. A special structure containing the AIK credential is created which is used in step three to activate the AIK by executing the TPM_ActivateIdentity command. So far, the TCG-specified protocol is not completely secure, since between steps two and three, some kind of handshake between PCA and platform is missing. The existing protocol could sensibly be enhanced by a challenge/response part to verify the link between the credentials offered in step one and used in step two, and the issuing TPM. The remote attestation process is shown in Figure 5.

Beside the attestation methods TC offers a concept to bind data blobs to a single instantiation and state of a TPM. The TPM_unbind operation takes the data blob that is the result of a Tspi_Data_Bind command and decrypts it for export to the user. The caller must authorise the use of the key to decrypt the incoming blob. In consequence this data blob is only accessible if the platform is in the namely state which is associated with the respective PCR value.
A mobile version of the TPM is currently being defined by the TCG's Mobile Phone Working Group [7]. This Mobile Trusted Module (MTM) differs significantly from the TPM of the PC world and is in fact more powerful in some respects. In particular, it contains a built-in verifier for attestation requests, substituting partly for an external PCA. Both TPM and MTM are a basis for application architectures. Trusted Computing affects the world of networked PCs but also heavily impacts the mobile industry.

REFERENCES


[15] ETSI EN 300 401: Radio Broadcasting Systems; Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers


