Technology, Implementation and Application of the Trusted Computing Group Standard (TCG)

Secure platforms provide new levels of security

Authors: Hans Brandl, Thomas Rosteck

Translation of the original paper from: Datenschutz und Datensicherheit, Vieweg, September 2004

Introduction

In recent years, the necessity, functionality and new possibilities of trusted computing as well as the fears and misgivings which it provokes have been a hot topic of discussion in many forums. In the meantime this technology has come of age, initial standards have been agreed upon and PCs are now equipped with it. What are the real issues here?

1 Purpose and content of the TCG specification

One of the as yet unresolved problems of widely used security applications is to protect the hardware platform against attacks on its integrity or modification of the security software. Typical published examples are the attacks carried out by CCC on the HBCI Homebanking System or the possible attack described in [Cre01] against a signature application which was even certified in accordance with the German signature law. Current approaches for solving this problem purely at the software level are by their very principle unpromising. As has since been amply confirmed from experience and security trends in the smart card world, a trusted and tamperproof security basis cannot be implemented using software-based solutions alone. This of course applies equally to host systems such as PC platforms. Although in the military and government sector there have been some attempts to develop purely software-based high-security systems, even there access to the appropriate hardware is greatly limited. An additional disadvantage is then that the functionality and flexibility of the operating system is generally very restricted. Today's widely used applications in a Microsoft Windows® dominated environment are based on convenience and are easy and intuitive to use. Consequently, flexibility and ease-of-use are also critical to commercial success in the case of secure and trusted operating systems.

Major companies in the PC sector have therefore joined forces and begun working to solve this problem with the aid of a new hardware approach and the creation of an associated industry standard. In 1999 Compaq, Hewlett-Packard, IBM, Intel und Microsoft established the Trusted Computing Platform Alliance (TCPA). The aim was to create Trusted Clients (e.g. PCs, but also PDAs or mobile telephones) in order to make important applications such as networks, communications and e-commerce much more trustworthy. At the same time, however, this standard was to be kept as open as possible in order to inform the technical and interested public in good time and to create confidence. The emerging Trusted Computing Standard employs a secure hardware structure whose main component, the Trusted Platform Module (TPM), is specified as an LSI security chip. This Standard is largely based on recent years' experience with high-security smart cards and their applications, important parts of whose architecture and security characteristics have been consistently adopted. Similarly to the way in which we use the smart card's cryptographic mechanisms to protect sensitive and confidential personal data as well as critical processes in a security environment, these functions can also be used in the TPM to ensure not only the integrity of a platform but also to protect its user data. To restate clearly:

The TCG Standard provides authentication and accreditation of the platform, **not of the user**. The Standard additionally permits secure storage of critical secrets such as keys.

For this task it accordingly includes, in addition to secure firmware principles and components, in particular hardware requirements of the type well-known from design principles for high-security crypto smart cards.

Inserting a secure TPM into the PC platform with standard PC modules does not, however, prevent intelligent attacks with hardware debugging and analysis tools. Although the TPM increases the resistance and security level of such a platform (TPM-protected data is virtually impervious to attack), it must be taken into account that 100% security is not achieved with the TC platform.

1.1 Standardisation: What is TCPA or TCG?

After the formation of the TCPA in 1999, the number of members rapidly grew to over 200. During and particularly at the end of the initial standardisation activities, however, it became clear that, at this size, the old TCPA organisational structure, which required e.g. unanimity for the decisions and Standards, was no longer efficient enough. In 2003 a successor organization, the Trusted Computing Group (TCG) [TCG01] was therefore created with a reformed and adapted constitution (e.g. only 2/3 majority for decisions), and the goals and activities of the TCPA were transferred to the new body. In addition, further opportunities for involving the interested public, over and above the information strategy, were created with a Liaison Program.

The TCG has since agreed three important specifications:

- Trusted Platform Module (TPM)
- PC Specific Implementation Specifications
- TCG Software Stack Specifications (TSS)

These parts set out the basic prerequisites for secure components on the new secure platforms. The corresponding member companies have simultaneously been investing considerable resources to ensure that the first implementations are available and that the first trusted motherboards with TPM or complete PC systems are ready for shipment. A rough overview of currently available TC-PCs can be found in [MCF01].

At the same time, however, standardisation work is continuing. In a total of around 20 working groups, from the Conformance Group on Mobile Communication to the User Authentication Group, the next application options and interfaces are being planned and standardised.

1.2 Security aspects in the TCG Specification

The generic TCG approach is producing new system structures: whereas until now security was to be achieved by means of additional levels of encryption or antivirus software, TCG begins at the very lowest level of the platform, and here right from the start of the booting operation of such a system, the TPM being trusted a priori as a certified HW security chip. At system startup an uninterrupted "chain of trust" extends from this lowest layer up to the applications. As soon as the lower level in each case has a stable security reference, the next layer can be supported on it. Each of these domains is built upon the preceding one and can therefore expect every transaction, internal link and device connection to be trusted, reliable, secure and protected.

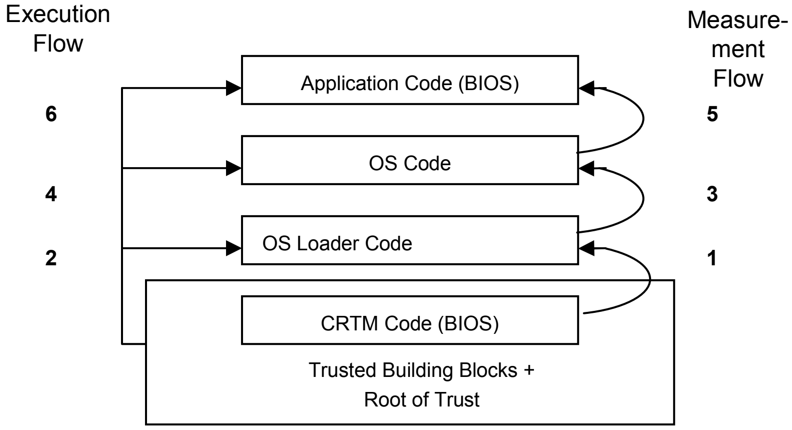

Fig. 1: Structure of the "chain of trust"

As a hardware security reference, the TPM constitutes the "root of trust" of the entire chain. Right at the start a check is performed to ascertain whether the signature (and therefore the constellation) of the platform components has changed, i.e. whether one of the components (disk storage, LAN connection, etc.) has been modified or even removed or replaced. Similar checking mechanisms supported by the TPM then successively verify e.g. the correctness of the BIOS, of the boot block and of the booting process itself, as well as the next higher layers at startup of the operating system. Throughout the startup process, but also later, the security and trust status of the system can therefore be interrogated via the TPM – but only with the platform owner's consent. However, this means that a compromised platform can also be securely identified by others and data exchange can be restricted to the appropriate extent. Trusted computing systems can create the conditions whereby for the first time modern, networked platform structures can also be significantly refined from the point of view of security and mutual trust.

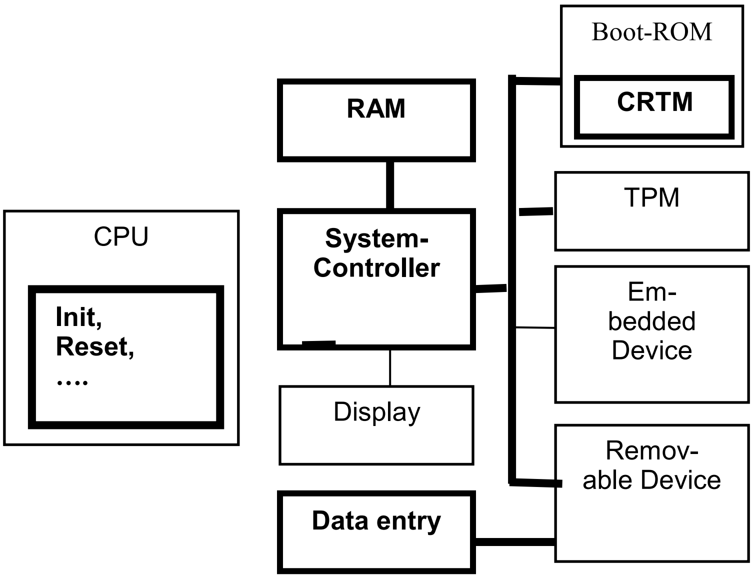

Fig. 2: Trusted platform: Trusted building blocks (core modules) accentuated

1.3 Protecting the user

Data protection aspects and user autonomy have been important principles of the TCG in defining the specifications. Results of discussions in the USA, but also in particular with the European Commission and the German government, have been incorporated as improvements in the latest version of the TCG Specification. The opinion of the EU as laid down in Article 29 (Data Protection) may be found in [EU01] and the TCG's response in [TCG05].

Essentially, platform owner control over the actions of the TPM is of primary importance.

2 Objects of the TCG Specification

A trusted platform as defined by the TCG consists of trusted hardware and software on the platform, and the connection and integration of external Certification Authorities (CAs, Trust Centers, already known from the "conventional" smart card signature solutions) in order also to enable the user and his platform to be identified to the outside world. The platform in turn logically comprises:

- Core Root of Trust for Measurement (CRTM).
  CRTM consists of the routines executed right at the start of booting of the platform (while the operating system is not yet available) in order to achieve secure startup conditions, essentially by measuring and monitoring the integrity of the boot operation. In technical terms, this is accomplished by forming hash values of the critical parts which are then sent to the TPM for checking. These functions have already been implemented in the more recent BIOSs (e.g. AMIBIOS8 with TCG support, [AMI01]). In accordance with the requirements of an open system, the signature references

required for this purpose are not supplied or preset either by the TCG or by any particular operating system manufacturer, but are the user's responsibility.

- Trusted Platform Module (TPM).
  The TPM is the central hardware security device (implemented as a chip) in which all the basic trusted operations and particularly the cryptographic functions are securely handled. Its structure corresponds approximately to that of the well-known high-security smart cards of the type used e.g. for digital signatures or also in payment transactions.
- Trusted Platform Support Service (TSS).
  TSS provides the operating system with a standardised high-level interface (API, referenced in C) to the TPM via which it handles the security functions of the OS or of applications.
- Initial Program Loader (IPL) as the link between BIOS and OS ensures the integrity of the OS.

However, it is generally true of all these procedures and methods that they are implemented in a data-protection-friendly manner. This means that they are not imposed on the user, for example, but that the owner of a TC platform must select during configuration whether to activate any of the many possible protection mechanisms. TC PCs ship with protection mechanisms deactivated. In a so-called opt-in procedure the user then installs his required security profile. This also implies that non-predetermined software parts, operating systems and other objects (such as network addresses) may be excluded by the application the TCG Standard.

2.1 TPM: hardware, software, functionality

In accordance with the TCG architecture, the TPM provides the security functions requiring particular protection and which are therefore also implemented in a secure hardware environment. Here too the privacy aspects are paramount: the TPM is designed as a passive part. The process has no means of actively influencing program execution of the central processor or the boot operation. It receives only control and status measuring data from the central processor which it processes, stores and reads out again from its secure structure, and feeds these results back to the central processor. Only there is the subsequence sequence of security procedures controlled using these results.

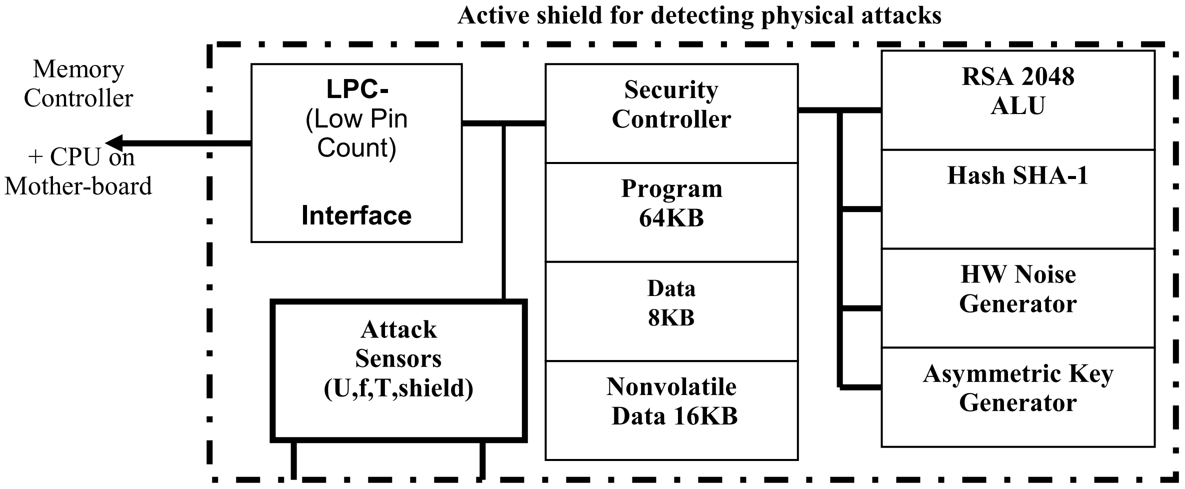

Fig. 3: Block diagram of Trusted Platform Module (TPM)

Only access to particular data (such as key material) is made dependent by the TPM itself on the presentation of appropriate authentication patterns.

The main security functions handled by the TPM are:

- **Protection of key material**
  The various key classes are stored in a protected manner in the TPM. The access method is selected according to key type (TPM-bound, migratable, signature, identity (AIK), binding keys).
- **System authentication**
  Authentication and validation of the platform to third parties.
- **Communication of the system's security status (attestation)**
  Trusted communication of the security-relevant (platform-user-defined) configuration.
- **Random number generator**
  Generation of genuine hardware-based random numbers for secure key generation.
- **File sealing**
  Binding of data to the system configuration and signing of the data when storing with the hash value of the configuration. Access to the data is then only possible if the configuration remains unchanged.
- **Secure saving of configuration changes in the Platform Configuration Registers (PCR).**
  Status changes are detected, safeguarded by the SHA-1 hash algorithm.

In addition, the TCG has also placed emphasis on some general, but at least equally important characteristics :

- Protection against attacks on the integrity of the TPM, particularly against physical attacks
- Inexpensive implementation in order to allow widespread use.
- Compliance with global export control regulations in order not to restrict international trade with TC platforms (PCs).
- And most importantly, an implementation which supports protection of the private sphere and self-determination of the user's data.

Skilful system design allows implementation with a minimal amount of cryptographic and security hardware in the TPM:

- Specialized crypto arithmetic unit for rapid computation of RSA cryptography up to 2048 bits.
- Key generation for RSA keys up to 2048 bits
- Hardware hash unit for the SHA-1 algorithm
- Genuine hardware noise generator as input for key generation
- Internal processor with the appropriate hardware for computing the critical functions (e.g. RSA with the secret key part) on a trusted basis in a secure environment.
- Monotonic, protected counter and time meter in order to prevent reply attacks.
- Nonvolatile memory (EEPROM) to retain the data even if the operating voltage is switched off
- Sensors and internal security structures (e.g. active screen over the top wiring layer of the chip) in order to detect physical attacks and counteract them.
- Low Pin Count (LPC) interface for connection to the mainboard processor.
- TPM self-test function

Extensive internal firmware implements the interface protocol defined by the Standard to the overlying layers of the host software (TSS) and uses the above hardware functions for this purpose. In addition, this firmware also checks and administers the various security sensors and reacts appropriately to detected physical tampering or alterations to the chip or its environment. The correctness of the implementation is checked and confirmed by an independent test institute by means of a complex ertification process (see 3.4).

2.2 TCG Software Stack (TSS)

Like any other hardware element, the TPM requires a special driver and service provider interface in order to enable it to be addressed from the operating system. This Trusted Platform Support Service (TSS) constitutes a security API which provides the TPM functions for the relevant operating system. TSS consists, at the lowest level, of the hardware-based device driver (in kernel mode) which initializes the interfaces and exchanges data with the TPM via the LPC bus. The next higher level consists of the System Service with:

- TPM Device Driver Library
- TSS Core Services
- TSS Service Provider

which handle the following functions:

- Coordination and management of multiple accesses to the TPM
- Converting the abstract API commands to the data stream for the TPM
- Readying the System Service (even if no user is active) for remote access e.g. by the system administrator
- A Cache Manager securely stores the data exceeding the memory area on the external mass storage, thereby providing a storage capacity for keys and security data which is limited only by the size of the disk storage. A similarly operating Authentication Cache Manager is additionally provided.

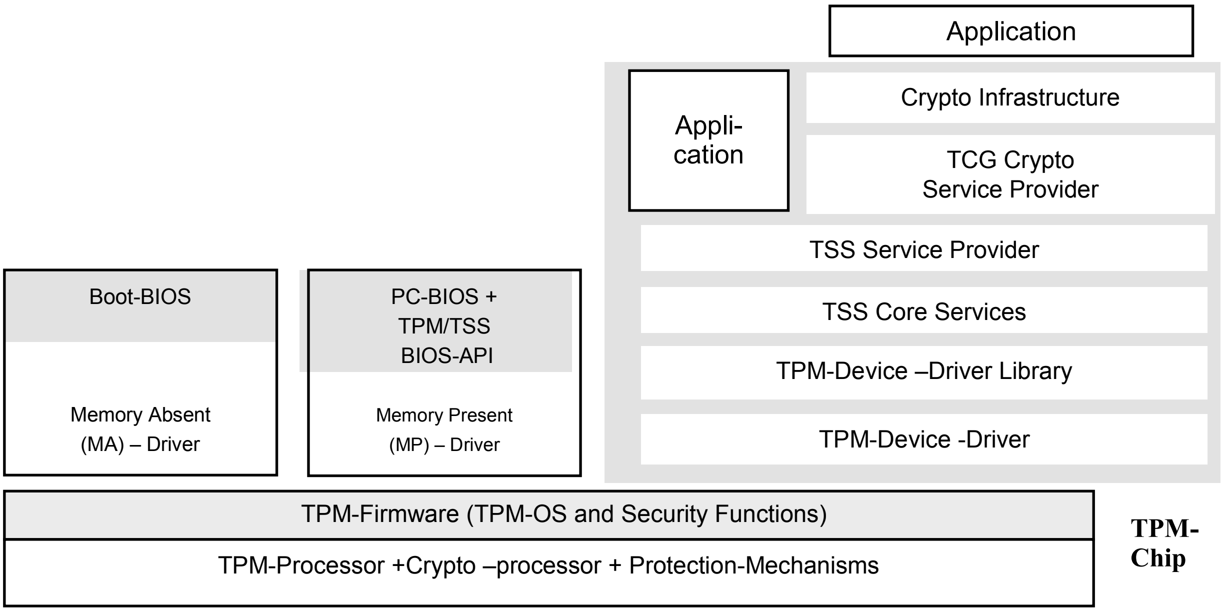

Fig. 8: Trusted Platform Support Services (TSS)

The operation and calls of the TSS are of course precisely specified by the TCG Standard, as its is only through precise and trustworthy implementation that the chain of trust between operating system and hardware TPM will remain stable.

TSS implementation naturally varies from operating system to operating system. As some of the sub-functions (e.g. lowest driver level) must be equipped with system rights, and the relevant OS characteristics also have to be taken into account, considerable know-how requirements are placed on the providers here. Normally the TPM manufacturer also supplies the TSS required for the relevant operating system.

2.2.1 Cryptographic interfaces of the TSS

Since the TSS, as an API, makes its security functions available to be operating system, it seems reasonable to provide this interface also for other security applications via an adaptation module, thereby enabling in particular secure storage and signature services of the TPM to be made available to the normal applications and the security level of these standard applications to be significantly increased. Although this functionality is not required by the Standard, it considerably increases the usability of the platform. Two usual implementations currently exist:

Microsoft Cryptographic Service Provider (MS-CSP)

Various application programs under Windows® (such as Outlook®, Explorer, Word ...) contain security functions such as encryption and signing and handle these functions via the so-called MS-CAPI (Microsoft Cryptographic Application Programming Interface) as a proprietary crypto interface. MS-CAPI can be directed to the TPM by accessing various security providers such as software modules, cryptographic tokens (smart cards, etc.) or again via the TSS. It is therefore relatively easy to port existing security applications already using MS-CAPI to the higher security levels of the TPM merely by selection of a different CSP.

PKCS#11

developed by the RSA is the most widely used universal crypto interface standard. It is used e.g. by the Netscape browser. Once again the conversion of the PKCS#11 security calls to the TSS-API facilitates the adaptation of existing standard applications quite considerably. Thus highly secure solutions can be achieved with minimal implementation cost/complexity by securely storing certificates for browsers in the TPM.

2.3 Secure platform: hardware equipment, Intel's LaGrande and AMD's SEM

As has already emerged from the deliberations concerning the implementation of trusted digital signatures, in addition to making the platform secure, a trusted interface to the user is also required. A trusted platform must of course also be able to satisfy the basic paradigm “What you see is what you get” (WYSIWYG). Although they TPM alone can check security statuses or digital signatures or even generate signatures, it cannot safeguard communication with the outside world or assume the security functions of the main processor. Additional security functions are therefore required in the other building blocks of a platform (secure input, WYSIWYG display, compartmentalized memory areas for the various process domains). The two major PC chipset manufacturers AMD and Intel are founder members of the TCPA and have since been engaged in incorporating the relevant security functions in their chip sets. Information particularly from Intel (LaGrande chip technology) concerning the current status and availability of such trusted PC peripheral devices is currently available [INT01]. Already obtainable or at an advanced design stage are [INT02]:

- Secure keyboard encoder with built-in encryption component [INT03] in order to forward the input data from the PC keyboard securely and without corruption to the processor for processing.
- WYSIWYG graphics interface [INT02] in order to ensure that it is really the output data of the relevant trusted application really appears on the screen, uncorrupted by omission or overwriting.
- Pentium CPU with additional address control registers and further protection mechanisms in order to reserve a protected memory area shielded from the other processes. This ensures that secure processes on the platform cannot be affected by malfunctions of other processes or do not themselves affect other processes.

3 Security mechanisms

3.1 Key and certificate chain in the TPM as starting point of the “chain of trust”

As the TPM Specification in accordance with the trust requirements of the TCG is completely public and accessible to all, someone could clone their own TPM on a processor in conformance with this Specification. If e.g. secure e-commerce processes are then transacted, the owner of this "special" TPM could easily modify the internal data to his advantage: such a module would certainly enjoy the full trust of its owner, but would be totally unsuitable for exchanging trusted processes. A trust structure has therefore been implemented which is already known from high-security bank cards (see MULTOS operating system [MULT01]):

Endorsement Key

At the end of TPM chip fabrication (after final testing), the manufacture generates a 2048 bit private/public key pair in the TPM, the so-called Endorsement Key. This is stored in such a way that the private key (PK) can no longer be read out, but can only be used internally in the TPM. The EK is additionally protected by a special certificate. The manufacturer thereby confirms electronically that this TPM has been produced in a trusted process by an inspected manufacturer and meets the requirements of the Specification. The trustworthiness of the entire TPM system is based for the most part on this process and the uniqueness of the EK. The user must trust the manufacture that the private part of the key is not stored anywhere, and that it is not accessible to anyone else. This aspect is also intensively tested as part of the security evaluation. In the case of qualified manufacturers such as Infineon, this fundamental process is performed in the same certified high-security area as for smart cards.

Indeed additional external storage of the EK by the manufacturer would also be pointless, as the TPMs are manufactured in an anonymous process, mounted in the motherboards in a purely randomly distributed fashion and then the PCs are likewise distributed to the customers in bulk. Tracking a certain TPM with its EK is therefore practically impossible.

Storage Root Key (SRK)

The SRK forms the root of a key hierarchy in which other lower-order keys, but also data (blobs), are securely stored, their trustworthiness therefore depending on the SRK. The SRK is automatically generated by the owner in a “Take Ownership” operation. If the owner of a TPM gives up this ownership, this also deletes the SRK and also makes all the keys protected by it completely unusable, which is welcome for data protection purposes.

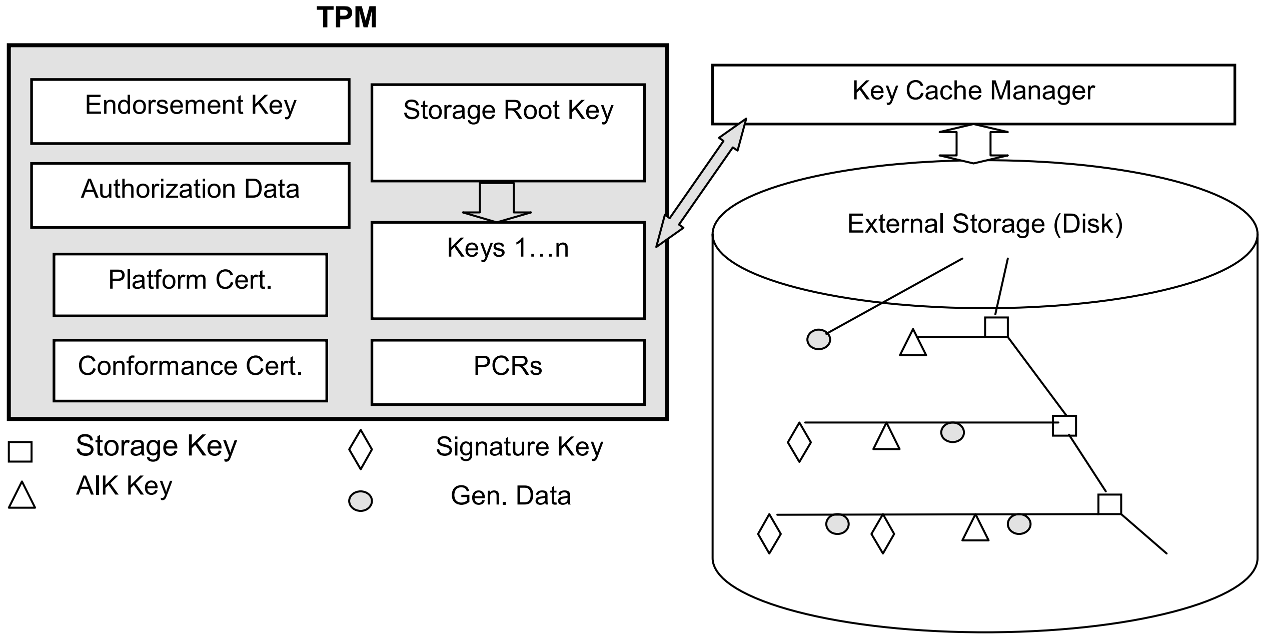

Fig. 5: Certificate chain

Attestation Identity Key (AIK)

The term attestation implies both authentication and integrity. Using AIKs and external Trust Centers, (even anonymous) identities can be created. AIKs are derived from the SRK and can also be subsequently created or deleted based on their use. Several AIKs are possible for each platform and for each user. Typical applications are:

- Server authentication
- Platform-bound digital contents (DRM)
- Anonymous identities in procurement and tender platforms

Direct Anonymous Attestation

In the latest TCG Specification V1.2, another attestation based on zero knowledge methods (direct proof) has additionally been defined, enabling platforms without external CA to mutually attest one another and improved anonymity to be achieved without an external third-party [INT05], [TCG01].

Certificates

Additional confidence in the correctness of the platform is created using further cryptographic certificates which are likewise stored in the TPM:

The **Endorsement Certificate** confirms that the TPM originates from a trusted source. It contains the public key (PK) of the EK and is used for forming the AIK.

The **Platform Certificate** is brought in by the motherboard/PC manufacturer and confirms that a valid TPM has been mounted in a correct platform. It is likewise used for forming AIKs.

The **Conformance Certificate** is issued by a test laboratory and confirms that the security functions of the TPM and motherboard have been positively checked and are compliant with the protection profile of the TCG.

The concatenation of these various certificates, credentials and keys in order to be able to make various security declarations constitutes a highly sophisticated logical system. The interested reader is referred to [TCG01] TCG Specification Architecture Overview, Sect. 4.2.5.

Key migration

As both platform-related and person-related keys (user keys) can be stored via the TPM, the need arises to transfer the user keys securely to other platforms. For this purpose the TCG has defined a set over rules under the term *migration*:

Non-migratable keys

(Bound to the platform)

Examples:

- EK: Endorsement Key of the TPM manufacturer
- SRK: Storage Root Key

These keys basically cannot be transferred to other TPMs as they are platform-specific. Under the rules, backup (maintenance) is possible as provided for in the Specification.

In the latest Specification Version 1.2 the EK can now be deleted in a particular process. Using the “revoke trust” procedure, the entire EK becomes invalid and is deleted, as are all the certificates and keys dependent on it. Using a likewise specific procedure, a new EK key pair can then be generated and the certificate chain reestablished. However, this method constitutes the exception and is conceivable for closed infrastructures. Establishing a new certificate chain for general use will involve very high costs.

Migratable keys

(transferable to other platforms)

Example :

- All the keys (if generated in a migratable manner) and data employed by the user and stored under the storage key.

Transport modes

Migration

(Transfer to other TPMs)

- For migration a special authorization process is used and the data material is transported in a password-protected container for security purposes. In practical terms this can be accomplished by a special migration server

Maintenance

(Backing up and restoring key material)
This feature is used for data/key backup in the event of a hardware defect (recommendation only). Implementation by backup server or e.g. smart cards

3.2 Activation and personalization of the TPM

The TPM is supplied deactivated in accordance with the trust principal of the TCG. It is up to the administrator or the individual user to put it into service (Opt-in Strategy for Privacy Control) [INT06]. This is done by calling the TPM management program of the TC PC:

- Initialization
  TPM self test, resetting the PCR registers and all flags, measuring the platform status
- Taking ownership
  The “Take Ownership” command takes possession of the TPM and basically creates a new Storage Root Key (see 3.1).
- Availability (Enabling)/ activation (Activated)
  The functions of the TP are activated.

In addition there are other commands for functions or status transitions :

- The Clear command clears the TPM completely apart from the EK and the platform certificates. This means that all operational keys are also no longer unavailable and any data still encrypted is no longer accessible!
- In order to prevent access to these functions by unauthorized persons, identification patterns (in the simplest case PINs) are either generated or interrogated for all these actions.
- The “critical” operations “Activation” and “Enable” additionally require the physical presence of the owner locally (e.g. entry via BIOS or by means of switches).

The opt-in procedure of the TPM (Privacy Control) [INT06] with its commands allows control by the owner/user from the point of view of data protection with granular gradation :

- Enable/Disable Ownership
- Enable/Disable TPM
- Activate/Deactivate TPM
- Enable/Disable PUBEK-Read (access to the public part of the EK)

3.3 Management of TC platforms

Whereas until now only the general logistical requirements have been created for handling standard PCs, new requirements arise for the handling of devices with unique identity and safety elements derived from it. In particular the porting and backup of rights, keys and identities require new terms of reference for use in the field. In the event of defects, it must be possible to migrate the sensitive data securely or re-import the backup data securely [INT07].

3.4 CC certification of chip and firmware

In order to ensure quality and confidence in the TPM module and also to reassure the user of this, it undergoes an official certification process in accordance with ISO15408 (Common Criteria, CC) similarly to the normal practice with smart cards. In the TCG a Protection Profile (PP) has been worked out for certification in accordance with CC EAL3 basic. Like all the other relevant TCG standards it is openly available on the TCG web site [TCG01]. In addition, hardening to CC EAL4 medium is already currently under discussion as an improvement. In any case, however, the prerequisite for a trusted system is successful evaluation and the existence of a valid certificate for hardware and software.

4 Operating systems and applications

Contrary to the assumption in some publications, the TCG standard is not bound to any operating system and in particular not to Microsoft. The Standard essentially governs trusted hardware platforms and consequently contains no requirements for the operating system. Only the open TSS-API is provided, which can of course be used by any operating system. Also the assertion made time and time again in this context that OSs or other software on a TCG platform must be certified (at considerable cost and therefore constituting an access limitation for using the technology) is inaccurate.[1] According to the Standard (see also 3.4), certification (in the sense of a security evaluation) is only necessary for the really relevant parts of the security core of the platform, TPM and TSS, in order to guarantee their trustworthiness to all users and OSs.

On the other hand, it is only an operating system on a TCG hardware platform that can make flexible trusted computing possible. The TCG Standard with its tamperproof and trusted hardware creates the basis to which the security mechanisms of the OS can relate. It is specifically for that purpose that the TPM provides its signature but also its secure storage functions.

Secure operating systems for TC platforms are mainly designed for separated compartments and domains. The basic considerations here are described e.g. in [TCG03], [INT04].

For the integration of and into an operating system the following activities are currently known:

4.1 Microsoft NGSCB

Best known publicly are the activities of Microsoft to integrate security functions directly into the operating system in its next operating system generation “Longhorn” using the TCG Standard [MS01]. Under the designation Next Generation Secure Computing Base (NGSCB, pronounced 'inscab'; formerly “Palladium”) work is underway to extend Windows® whereby trusted execution environments (known as NEXUS) are created in secure compartments. This approach could be very distantly compared with the well-known DOS box. This will make it possible, depending on user requirements, to support secure and trusted processes in the NEXUS compartments while continuing to support traditional applications. The user shall therefore have the opportunity to:

- keep data and applications in protected compartments
- use secure data paths between keyboard, processor and display
- continue to support existing security and processing environments and to reinforce them

As is to be expected, the challenges here are not only to create a new, secure operating system part, but above all to harden the previously used input and output channels which actually have to be at least partially shared by NEXUS. According to information currently available, Microsoft is currently engaged in using the learning effects from the previous development and revising its architecture.

[1] This assertion resulted from the lack of understanding and therefore the confusion of the two uses of the term “certificate”:

1. Cryptographic certificate for the digital signature of data or programs
2. Confirmation of successful checking of a process or software by a testing institute (e.g. Common Criteria)

4.2 Open Source

Whereas public discussion concerning TC applications and characteristics has focused on Microsoft, in the area of Open Source (specifically Linux) the first deployment and application examples have already emerged. Add to this further activities whose descriptions may be found on the Internet:

- IBM has put the lowest driver level of its TSS stack as an Open Source Linux implementation on the Net [IBM02]. Similar activities of other providers will follow.
- The open TPM-based software "Enforcer" [IBM01] monitors the integrity of programs at startup and is intended primarily for servers.
- At the Royal Holloway University London intensive research is already being carried out into TC-supported secure Linux kernels [Lam01] and the linking of TC and identity management.
- The Institute for Applied Data Security at University of Bochum, Department of Electrical Engineering has already realized a Trusted Bootloader for Linux (Trusted GRUB [Grand Universal Bootloader]) and also develops a Linux driver for the Infineon TPM [ADS01]

We assume that many more such activities exist and these developments are set to increase significantly in the near future.

4.3 Applications

Independently of the operating system activities, standard security applications based on the TCG Standard are already widespread. In most cases existing programs and functions are adapted to the TSS of the TPM using the standard crypto interfaces CSP and PKCS#11. Virtually every TC-PC supplier is now providing standard security programs such as file encryption, single sign-on, secure log-in as part of his package in order to demonstrate the possibilities of the secure computer even to the "security novice". In addition, there are an increasing number of security applications from a wide variety of manufacturers [TCG02].

5 Functionality and application

5.1 Security functions for supporting the operating system and applications

One of the essential elements of the TCG Standard is the TSS which, as the API to the TPM, provides the security services for the platform operating system and the application programs. Whereas the TSS native API is responsible for the execution and tasks of the operating system, for the applications there are the well-known universal crypto interfaces such as :

- MS-CAPI (Microsoft Cryptographic Application Programming Interface) and
- PKCS#11

It is therefore possible, for example, to securely implement the known cryptographic functions in hardware or securely administer key material and other sensitive data. Supported standard programs include :

- Microsoft programs with integrated security components, such as Outlook® and Explorer
- Netscape Communicator

TPM and TSS can create a separate, individual security environment for each user.

5.2 Integrity checking

With the "Taking Ownership" procedure for TPM management, the owner can establish the trusted status e.g. of a PC or notebook. This enables the system, during the next boot operation, to compare the current status with the reference status stored in the TPM. If these values (stored in the PCR register) agree, the system is deemed to be trustworthy. Any modification of important parts due to attacks or a virus can be detected in this way and the user can take appropriate action.

5.3 Authentication

As the TPM can also simulate the basic smart card functions, it can also be used for authentication tasks and access control. The following application example is conceivable:

For secure e-commerce or access to a protected web page, a key pair or cryptographic certificate can be stored in a trusted manner in the TPM. This means that it is possible both to identify oneself uniquely to the other party (e.g. bank) and use the same mechanism also for encrypting the connection.

Ideal applications in networks are e.g. also secure remote control and monitoring of firewalls and VPNs.

5.3 Benefits for system administrators

System administrators can unambiguously identify the different devices in their networks with the aid of a TPM. New devices are reliably booked into network management, unknown or changed devices can be clearly detected. This enables security policies to be further automated and implemented in a controlled manner.

Through the use of known remote access server procedures, not only the users' authentications (name, password, smart card, biometrics) but also the platform used can be identified. The network can check, for example:

- The user's access rights
- If a company notebook known to the system is being used
- If the notebook has trusted status

If these checks are passed, the security policy can permit unrestricted access. If it is the correct user but e.g. an unknown PC, operation with restricted rights (e.g. for file access) is possible.

5.4 Anonymization e.g. for provider and procurement platforms

By means of the attestation ID functions, a TC platform can appear under an anonymous identity in order e.g. in the case of procurement and auction platforms to issue anonymous bids without the buyer being influenced by the bidder's identity. An external, neutral and trustworthy Trust Center must hold the connection of the anonymous identity to the real identity and, once the bid has been accepted, provide information about the mutual identities, therefore enabling the contract to be transacted.

5.5 Interaction with smart cards, biometrics, etc.

It is often erroneously assumed that TPM-based TC platforms would replace smart cards or other authentication methods. TC is, however, designed to supplement these functions. If a person authenticates himself using a cryptographic token or biometric method, the target system always requires a secure reference against which the authentication data can be checked. In today's systems, this data is mainly stored on a special server or, in the case of standalone systems, hidden deep in the memory. TPM also makes it possible to store any reference data securely and in a protected manner. This means that for the first time even high-security authentication processes can run on normal standalone systems. The processes and protocols necessary for this purpose are currently being worked out by the TCG's Authentication Workgroup [TCG01].

6 Future applications

Although the TCG began its activities with PC security in mind, the idea of the secure platform is transferable to other devices and applications. Within the framework of the TCG there now exist workgroups for a wide variety of application fields. Topics of discussion include:

- PDAs and smartphones
  PDAs now have similar features and functions to PCs, are operated continuously on the Internet and are at considerable risk of theft or loss due to their portability. The operating systems which they typically employ mainly have no or only minimal security functions. Losing a device generally results

in all the data contained in it being compromised. TPM and its use in the OS can bring about a considerable improvement here by means of implicit authentication and encryption methods.

- Mobile communication applications
  Modern devices such as UMTS are in operation and connected to the Internet 24*7h, and so far no particular security precautions have been taken. With TPM not only can data security be improved, but the applications possible can also be significantly increased. In particular the possibility of securely storing certificates in the device makes new trusted applications possible. With a TPM security core, the mobile phone suddenly becomes a security terminal for m-commerce or, by using the existing keyboard and display, a secure Class 3 terminal for signing documents or for e-banking. Even the increasing risk due to harmful software (a virus/worm which dials the emergency number is now quite conceivable) can be better countered using a TC-based operating system.
- Communication (WLAN security, network remote access ...)
  Particularly of late, the topic of security for external network accesses has gained increasing importance. Of particular interest here is the protection of WLAN systems. Now that the first generation systems have been superseded by much more sophisticated protection mechanisms, here too a requirement is arising for secure storage of key material and for storage of device certificates for identification. Here TPM offers the possibility of integrating security into the devices in a trusted manner, not only for the WLAN air interface but also for network accesses (RADIUS, DIAMETER).
- Equipment security and integrity
  For protecting high-value assets against attacks on their integrity or unauthorized modifications, a large number of applications present themselves. These range from protecting product features of cars such as engine control, or of value-related parameters such as mileages, through to protecting system controls e.g. in chemical plants. The discussions here are only in their infancy, but even here platform integrity is opening up new possibilities.
- Digital rights management
  DRM to it is a technology which can be used both for management of corporate data (company documents or the secure organization of document and workflow management systems) and for so-called content (music, videos, games, etc.). With minimal expense, security areas can therefore be created on the terminals, enabling the distribution and management of usage rights to be checked in a fair and comprehensible manner. Although its use for DRM has hitherto weighed heavily on the discussion concerning TC, on the other hand many positive application options are emerging, as it can be the basis for new business cases and therefore for offering content in the network. Other DRM standardisation groups such as Open Mobile Alliance (OMA) with DRM2.0 for mobile communications can base their work on TC functions.

7 Further reading

- The entire Specification, concepts and architectural considerations of the TCG can be openly found on the TCG web site [TCG01]. Typical but also necessary for specifications, however, is their considerable size (a total of around 500 pages) and the dry-as-dust presentation which can be quite off-putting [2].
- The basic objectives and principles are described in “TCPA Design Principles” [TCG04]. It is recommended that at least this overview document of the TCG be worked through directly.
- Security experts from HP who were involved in the Specification have written the book on TC [Pea01]: TCPA Design Philosophies and Concepts. This book is the best introduction to the TCG philosophy, is well explained and is best related to applications. Unfortunately the very latest revision of the Specification (V1.2) is currently not yet included.
- [IBM03] examines the misinformation, assumptions and incorrect statements in the TC discussion.

Summary

In order to establish secure and trusted computer platforms on a widespread basis, the relevant PC companies have set up the Trusted Computing Group as a standardizing body. The new open TCG Standard for trusted hardware provides a starting basis not only for secure PCs but will also enable

[2] Unfortunately there was therefore often a lack of well-founded information from the Specification in previous TC discussions.

the new generation of personal communication devices, servers and industrial controls to be provided with more sophisticated security features.
Data protection and platform user autonomy have been basic design principles for the Specification.
The TCG Standard is not bound to particular operating systems or host software and therefore allows a wide, independent distribution of secure platforms and their advantages.
Well-considered use of this technology will make possible completely new secure and trusted functions for security systems.

References

[ADS01] Applied Data Security at University of Bochum, Department of Electrical Engineering. Trusted GRUB: http://www.prosec.rub.de/trusted_grub.html

Linux Kernel-Module for the Infineon Trusted Platform Module SLD 9630 TT: http://www.prosec.rub.de/tpm/index.html

[AMI01] AMIBIOS8 und TC: http://www.ami.com/support/doc/AMIBIOS8_TCPA_whitepaper.pdf
[Cre01] Cremers, Spalka, Langweg: 7. Deutscher Sicherheitskongress 2001: Vermeidung und Abwehr von Angriffen trojanischer Pferde auf digitale Signaturen: http://www2.hig.no/~hannol/research/bsi01t.pdf
[EU01] EU zur Trusted Computing Group http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp86_en.pdf
[IBM01] IBM-Linux Application Enforcer (Checking of programs during the loading) http://enforcer.sourceforge.net/
[IBM02] IBM: GPL-Sourcecode of the IBM TPM Driver http://www.research.ibm.com/gsal/tcpa/tpm-1.1b.tar.gz
[IBM03] IBM: Watson Research - Global Security Analysis Lab: TCPA Misinformation Rebuttal http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf
[INF01] Infineon: TPM Produkt Information http://www.infineon.com/TPM
[INT01] Intel: La Grande Technology and Safer Computing Overview: http://www.intel.com/idf/us/fall2003/presentations/F03USSCMS16_OS.pdf
[INT02] Intel: La Grande Technology Architecture http://www.intel.com/idf/us/fall2003/presentations/F03USSCMS18_OS.pdf
[INT03] Intel: Trusted Mobile Controller Architecture http://www.intel.com/idf/us/fall2003/presentations/F03USMOBS147_OS.pdf
[INT04] Intel: Software for LaGrande Platforms: Impact to Software Development Process http://www.intel.com/idf/us/fall2003/presentations/F03USSCMS20_OS.pdf
[INT05] Intel: Privay method for Assuring Trust http://www.intel.com/idf/us/fall2003/presentations/F03USscms19_OS.pdf
[INT06] Intel: An Opt-in Strategy for a Safer Computing Platform http://www.intel.com/idf/us/fall2003/presentations/F03USscms156_OS.pdf
[INT07] Intel: Recovering from Computer failure if TPMs Go Bad http://www.intel.com/idf/us/fall2003/presentations/F03USSCMS25_OS.pdf

Intel: TCG Credentials: Their role in the Trusted Infrastructure and Manufacturing http://www.intel.com/idf/us/fall2003/presentations/F03USSCMS157_OS.pdf

Intel: Trusted Platform Module: Impact to Manufacturing and Testing http://www.intel.com/idf/us/fall2003/presentations/F03USSCMS180_OS.pdf
[Lam01] Lambroux: Thesis Royal Holloway University of London (RHUL): TCPA enabled Open Source platforms http://www.crazylinux.net/downloads/projects/TCPA/TCPA_thesis.html
[McF01] Tony Mc Fadden: TPM PC Vendor Overview: http://www.tonymcfadden.net/tpmvendors.htm
[MS01] Microsoft: Microsoft's Next Generation Secure Computing Base (NGSCB) http://www.microsoft.com/NGSCB
[MUL01] MULTOS Betriebssystem: http://www.multos.com
[Pea01] Siani Pearson (ed.): Trusted Computing Platforms: TCPA Technology in Context, Prentice Hall PTR2003

[TCG01] Trusted Computing Group Website: http://www.trustedcomputinggroup.org
[TCG02] TCG Press papers: https://www.trustedcomputinggroup.org/press
[TCG03] TCG: Writing trusted Applications:
https://www.trustedcomputinggroup.org/downloads/Writing_Trusted_Applications_TCG.pdf
[TCG04] TCG: Design principles:
https://www.trustedcomputinggroup.org/downloads/tpmwg-mainrev62_Part1_Design_Principles.pdf
[TCG05] TCG: Answer to the comment of the EC:
https://www.trustedcomputinggroup.org/press/feb_6_art_29_report_QA.pdf