ARTICLE 29 Data Protection Working Party

11816/03/EN
WP 86

Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG group)

Adopted on 23 January 2004

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 14 of Directive 97/66/EC.

The secretariat is provided by Directorate E (Services, Copyright, Industrial Property and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.
Website: www.europa.eu.int/comm/privacy

Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG group)

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to articles 12 and 14 thereof,

has adopted the present Working Document:

Background and future perspectives for trusted computing platforms

The concept of trusted computing platforms originates from the computer industry's observation that the current personal computer model is not conducive to guaranteeing security, as demonstrated by virus attacks, the possibility of spying on data being input, pirating of software and works of art, etc.

This concept is increasing in importance at the same time as forecasts of Internet use predict a decline in the relative importance of the Web – the public part of the Internet characterised by a large number of unsecured transactions – with private areas where security concerns will be paramount taking up the slack.

As the foundations of security are still to be laid down, electronic signatures and their legal development are attempts to deal with issues raised by transactions on the network, while trusted computing platforms are intended to deal with issues related to the ownership, integrity and, where necessary, confidentiality of intangible goods, and to controlling their use in terms of both software and hardware. Not all of the various building blocks of these new, highly sophisticated architectures have yet been defined, tested or are even available. However, it is clear that the level of security for such platforms will not be higher than EAL3, as defined by the common criteria. By way of comparison, the required level for bank cards which incorporate smart chips is EAL4 or EAL4+.

Past attempts to increase security by identifying hardware components (such as Intel's Pentium III, which included a unique universal identifier) faced setbacks because of the risks to privacy. Having learned their lesson, researchers turned to reconciling various

[1] Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/privacy/law_en.htm

ways of using sophisticated cryptology techniques, taking an approach which focused on protecting privacy and personal data. For this reason, PET (*privacy enhancing technologies*) applications such as individual digital safes or virtual identity managers are proposed for trusted computing platforms. However, up to now, no viable economic model can be provided for these functions, which would be based on dedicated chips.

As a result, the applications are still relatively undeveloped, and the main focus is on digital rights management applications.

However, it should be pointed out that the concept of property in the information society is in flux and the subject of heated and premature controversy. It is a long way from achieving either legal or economic stability. Moreover, the role that public areas are to play will probably have to be (re)considered.

In addition, the concept of property is clearly part of the specifications for the Trusted Computing Platform Alliance (TCPA) and the Trusted Computing Group (TCG group) where the roles of users and administrators are clearly differentiated. It is administrators who are responsible for defining and limiting both the technical and practical rights of the users, which clearly raises questions of balance.

Looking at future possibilities, Digital Rights Management (DRM) systems may be up to the task of defining and, to a point, making access, or even the use of personal data under contract, secure on an individual basis. If such applications are not yet mature, it is because they only exist in a few research laboratories and require the support of established law. Computing platforms capable of administering these rights will be the same as the trusted computing platforms which are the subject of this report.

The Working Party's approach and methodology

The Working Party follows with interest the developments concerning Trusted Computing and, in particular, the work done by the Trusted Computing Group, an ad hoc industry consortium drafting specifications for a new class of hardware security chips called Trusted Platform Modules (TPM).

While being aware of the fact that the TCG group focuses mainly on the definition of certain components of a platform rather than on the platform as a whole, the Working Party realises that the building blocks developed by the TCG group (and particularly the TPM) will have important consequences for the future functioning of platforms (currently PCs and servers, but also, in the long term, PDAs, mobile phones, etc) operating in a fully interconnected world.

The international press also has given much attention to this development, as a result of not only the promotional activities of the TCG group but also of the important contributions to the discussion by some Data Protection Authorities[2] and relevant academics[3].

The Working Party decided to enter into dialogue with the TCG group and, during 2003, held several meetings of its Internet Task Force with TCG group representatives to discuss the technical and legal aspects of the TCG group specifications.

[2] Reference to documents of CNIL, Office of Alexander Dix…

[3] Reference to work of Ross Anderson.

The Working Party is pleased to observe that the TCG group has taken on board several of its suggestions in version 1.2 of the specifications and has created a best practices group to make recommendations on data protection-related issues.
It is the intention of this document to point out some of the matters that deserve additional attention and should be further considered by the TCG group.

The evaluation of the TCG group work made in this document is limited by a number of constraints linked to the current level of development of the specifications. At the moment it is still impossible to know how the specifications will be used, which applications or operating systems will be developed, which actors will be involved, which business models will be put into place and so forth. Another element of uncertainty derives from the fact that the specifications neither oblige to use all its elements nor oblige to implement the new features included in version 1.2. Not all functions defined in the version 1.2 TPM specifications will be implemented in every platform-specific component.

Therefore, this issue will require further work in the future; the Working Party will follow the developments, especially concerning specific applications.

What is the TCPA/TCG group?

According to own statements of this group, the mission of TCG group is to develop and promote open, vendor-neutral, industry standard specifications for trusted computing building blocks and software interfaces across multiple platforms. TCG group is incorporated as a not-for-profit corporation with international membership that has adopted the TCPA specifications as a starting point.

The group, an ad hoc industry consortium, includes many important players in the technology field not only from the computer world but also from other disciplines. It is for instance interesting to note that Sony has joined this group[4].

Trusted Platform Modules (TPM) based on TCPA specification 1.1b are presently available from three vendors: Atmel, Infineon and National Semiconductor. Some compliant PC platforms are shipping now: IBM ThinkPad notebooks and NetVista desktops. The industry hopes more will be available soon.

TCG group drafted specifications for security chips (TPM). These chips are targeted at the everyday computing, and so, according to the industry, the focus of efforts is on securing hardware platforms. The main objectives of the TCG group are authentication and increasing security levels. Furthermore TCG group products will help to realise Computational grids[5].

The TPM chip has the following functionalities:

[4] The Trusted Computing Platform Alliance, or TCPA, was originally formed by Compaq, HP, IBM, Intel and Microsoft. Presently, the promoters of TCG group are AMD, HP, IBM, Intel and Microsoft but additional promoters are anticipated. Current contributors, including some Europeans, are ATi Technologies, Atmel, Broadcom Corporation, Comodo, Fujitsu Limited, Gemplus, Infineon, Legend Limited Group, National Semiconductor, Nokia, MTRU Cyrptosytems, nVidia, Phoenix, Philips, Rainbow Technologies, Seagate, Shang Hai Wellhope Information, Sony, Standard Microsystems, STMicroelectronics, Texas Instruments, Ultimaco Software AG, VeriSign and Wave Systems. Additional companies, such as Sun Microsystems, have expressed interest and intention to join.

[5] Computational Grids enable the sharing, selection, and aggregation of a wide variety of geographically distributed computational resources (such as supercomputers, compute clusters, storage systems, data sources, instruments, people) and presents them as a single, unified resource.

- public key functions: key pair generation, public key signature, verification, encryption and decryption

- trusted boot functions: Platform Configuration Registers (PCR) store hashes of configuration information throughout the boot sequence. Once booted, data (such as symmetric keys for encrypted files) can be "sealed" under a PCR

- initialisation and management functions: allow the owner to turn functionality on and off, reset the chip, and take ownership. The new version of the specifications allows the owner to delegate a number of the functions to the user.

TPM technology makes it possible to implement security policies.

The development of specific applications is still in its first phase. Some examples of possible applications are Digital Rights Management (DRM)[6], the Next generation secure computing base (formerly known as Palladium) by Microsoft and the Intel LaGrande technology. At this moment it is impossible to have a full perspective of what possible uses of TCG group specifications might exist in the future.

The Working Party would like to emphasise that, as it has been stated in previous documents[7] regarding similar situations, the TCG group bears responsibility at least as far as the technical development of the project is concerned. They should also ensure that the specifications and protocols they design allow those using them to comply with the Directive[8].

Both those who design technical specifications and those who actually build or implement applications or operating systems bear responsibility for the data protection aspects, although at different levels. Those who build, commercialise and use the applications bear responsibilities as well, especially organisations that process user data, as they will normally be the last one in the chain and the ones who interact with the user.

Legal framework

The Article 29 Working Party would like to emphasise that the work of the TCG group should take into account the requirements deriving from the existing legislation. Directives 95/46/EC and 2002/58/EC are the main instruments regarding data protection in general and data protection in electronic communications respectively. In addition to that, the provisions of the electronic commerce[9] as well as the electronic signatures[10] directives should also be considered in this context.

[6] The Working Party will do some work in this field in the near future.

[7] See for instance the Working Document on on-line authentication services, adopted on 29 January 2003, WP

[8] See also Directive 99/5 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, Official Journal L 091, 07/04/1999.

[9] Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Official Journal of the European Communities, 17 July 2000, L 178/1 to 178/16.

[10] Directive 1999/93/EC on a Community framework for electronic signatur*e*s, Official Journal of the European Communities, 19 January 2000, L 13/12 to 13/20.

Many of the principles of the data protection directive have significant implications in this context. The Working Party would particularly like to emphasise the importance of the principles of proportionality and of the need to collect and process data. These principles imply that, in striking a balance between the fundamental rights of data subjects and the interests of the different actors involved, as few personal data as possible should be processed.

These principles have implications on the design of the new protocols and devices: while technology is *per se* neutral, applications and design of new technological tools should be privacy compliant by default[11].

The Working Party is aware of and supports the work being undertaken by the European Commission in the field of Privacy-Enhancing Technologies and encourages the TCG group to continue applying the PET philosophy in the further steps of its work.

Some reflections concerning the data protection implications of the TCG group work

As the technological environment is currently under discussion, the Party would like to limit itself to making a few general observations suggested by the basic guidelines currently accepted across the industry.

- Environment of use

Any attempt to analyse the data protection implications of the TCG group work should distinguish between the different environments in which TCG group compliant platforms can be used:

- In business environments the proposed infrastructure could be useful for enhancing security; especially in corporate networks. It is important to note that according to the TCG group consortium businesses are the first targeted consumers/users of the system.
- In consumer environments it is less clear where the benefit for the user lies. TCG group might deliver some improvements from the user perspective concerning protected storage and the opportunity to use digital pseudonyms for transactions. But TPM-based applications could be used to the disadvantage of users as well, for instance by the content industry in order to regain the control of the distribution and use of digital content (including software) that they have lost with the advent of Internet and peer-to-peer applications.

- Freedom of choice regarding use of TPMs

The TPM specifications make a distinction between the role of the owner and the role of the user. This distinction does not have any consequences in the private sphere as an individual would then be both the owner and the user, but it can raise some issues in corporate environments.

In the corporate environment an individual worker would be the user while the employer would be the owner. He may take a number of decisions that affect the individual employee and the amount of data concerning the individual that is processed. The owner (employer) bears responsibility in this case for the provision of information to the users and for an adequate protection to the individuals.

[11] See in that respect Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6, Adopted on 30 May 2002, WP 58

Version 1.2 of the specifications has brought with it some improvements in this situation by adding a delegation system for decisions regarding the use of various TPM functions, but the owner still has ultimate control and can decide whether to delegate certain key functions or not. As this is the case, it cannot be claimed (as some of the TCG group companies do on their websites or in their official statements) that individuals have the free and full choice of whether they accept the use of the system.

At the moment the possibility for the user to decide whether or not to use a platform with a TPM exists outside the corporate environment, although one can wonder how long this situation will last. The use of TPM, promoted by such a strong representation from industry, is likely to become a de facto standard, a necessary feature to participate in the information society. This could have consequences not only in the field of data protection, but also regarding other human rights aspects such as the freedom of speech.

- Informing users

In practice, the technical complexity of TPM-based systems makes it difficult to assume that the average user will be able to understand the information about the system and make informed choices as to their use, understanding implications. The Working Party encourages the TCG group to ensure that simple and understandable information is provided to users and, even more important, to make sure that sufficient protection is provided in all cases, not depending on steps that the user has to take.

- Security features

The TPM specifications include features that reinforce security. Security and integrity are of course important aspects, which are also relevant in the context of the data protection directive. The Working Party wonders however if the level of security could be “tuned” to specific uses of the system on a case-by-case basis. After all, security should be proportional to the risks at stake and these risks will vary depending on the situation: for instance, when a user wants to access his medical file on-line more security will be required than when an individual wants to register at a website that provides news services.

- Data protection using outside certification or anonymisation

In order to limit the transmission of identifiers and thus also the compilation of user profiles by third parties, the TCG group makes it possible for a trusted third party to certify users’ identities and confirm them to their correspondents without actually revealing the identities. This trusted third party (called a Privacy Certification Authority by the TCG group) is also one that needs detailed consideration. Concentration of data always involves additional risks and therefore sufficient precautions should be taken. As for TPM, there are scenarios in which a single trusted third party controls huge amounts of authentication information.

Version 1.2 of the specifications makes it possible to do without a trusted third party by using the “Direct Anonymous Attestation” (DAA) feature, which enables users to create Attestation Identity Keys (AIK) without presenting Endorsement Keys (EK), which are unique identifiers[12]. The Working Party considers this to be an improvement but notes that the choice between the trusted third party and DAA will be made by the applications. The current specifications will still allow both functions.

DAA is therefore an additional possibility, not a standard feature of the system in all cases. The Working Party feels that the introduction of the DAA functionality[13] is an improvement, but would like to reiterate that, in the cases where it is possible to establish a link with the identity of the user or to create profiles of the users, one can no longer talk of anonymity[14]. It encourages TCG group to promote the use of this functionality in the most privacy-friendly or enhancing manner: using random identifiers as much as possible and, where revocation and identification are necessary, restricting the use of names to as short a time as possible.

The Working Party wishes to stress the importance of the role that trust plays within TPM-based systems. Trust should exist through the whole chain of those involved, from the designer of specifications to the seller of applications and the deployer of the system. Data protection should be considered in all stages of the process.

Elements that deserve further consideration in the guidelines and best practices to be elaborated by the TCG group

The Working Party feels it would be very useful to create a best practices group within the TCG group to deal with the data protection issues at stake and develop guidelines and best practices concerning them.

The role of this group will be crucial for an implementation of the TCG group specifications that respects privacy and freedoms. The Working Party invites this group to deal in particular with the following matters:

- The role of the trusted third party (Privacy CA): who will be the trusted third party and what role will they play? The best practices group could produce some guidance as to the safeguards that should be put in place. If it is established in Europe, the trusted third party will have to comply with data protection rules. The rules of the e-commerce and e-signature directives will also have to be taken into account.

- The use of the DAA functionality: the best practices group should promote random identifiers as the first choice, unless there is a specific need to use names. Where a name is needed, use should be short term to prevent long-term profiling of users. Users should also be fully informed. The best practices group could elaborate a number of examples of different services and the way in which DAA could be used in each context to illustrate the issues at stake and identify the key questions that should be dealt with.

- The provision of information to the users: information should be complete and easily-understandable and provided to the user at different levels. There is a chain of responsibility from the designers of the specifications to the manufacturers, the developers of new operating systems or applications, those who commercialise them,

[12] The DAA is an alternate method to the trusted-third-party approach to establishing the validity of an AIK. It uses the zero-knowledge proof cryptographic technique and establishes the AIK validity without exposing the EK credential to the identity provider.

[13] The lack of practical experiences with the functioning of zero knowledge proof systems makes it also difficult to assess how the DAA will work in practice.

[14] See recital 26 of the preamble to the data protection directive.

etcetera. The use of the TPM should be transparent to the user, especially at application level.
The Working Party is concerned that the technical complexity of TPM-based-systems might make it very difficult for the average user to understand the implications and consequences of the use of certain features of the system and urges the TCG group to produce information packages in clear and plain language allowing a full understanding of the technology and the responsibilities.

- The need for control and enforcement through the process: the Working Party is aware of the fact that the TCG group can not fully control the privacy compliance of the applications but feels it would be very useful to include in the systems mechanisms to control use of the specifications. During the dialogue with the members of the TCG group the creation of a logo or certification programme for compliant-products has been proposed.
The Working Party wishes to encourage the TCG group to explore such possibilities and to develop recommendations and guidelines to motivate companies to use the specifications in a way that respects or even enhances privacy and liberty. Special attention should be paid to the specific contribution made by European legislation in this field.

Conclusion

The Working Party is pleased to observe that the TCG group has taken on board several of its suggestions in version 1.2 of the specifications and has created a best practices group to make recommendations on issues related to data protection, privacy and liberty. It invites the TCG group to reflect on the issues raised in this paper and build in the system not only privacy-compliant but also privacy-enhancing features.

At this moment, the TCG group specifications have hardly been used in practice and may undergo changes in the future. Some of the possible uses of this technology have not been identified yet and many questions will be decided at the level of the applications. New functionalities should be put in place in other platforms rather than PCs, such as mobile phones, PDAs and so forth. There is therefore great uncertainty at the level of the services and applications.

The Working Party will therefore continue to follow developments in order to make sure that the requirements of the Directive are taken into account. It invites the TCG group to report regularly to the Working Party about further progress and development of applications and in particular about the work done by the best practices group and the Board of Advisors.

Done at Brussels, on 23 January 2004
For the Working Party
The Chairman
Stefano RODOTA