



EUROPEAN COMMISSION

Information Society and Media Directorate-General

Audiovisual, Media, Internet

Internet; Network and Information Security

## STAFF WORKING PAPER

### *Trusted computing: a public policy perspective*

- Version 1.0 dated 12/02/2009 -

#### DISCLAIMER

The views expressed in this paper do not necessarily represent the position of the European Commission.

#### TABLE OF CONTENTS

<b>O.</b>	<b>MANAGEMENT SUMMARY .....</b>	<b>2</b>
<b>I.</b>	<b>INTRODUCTION .....</b>	<b>3</b>
<b>I.1</b>	<b>TOWARDS A SECURE INFORMATION SOCIETY .....</b>	<b>3</b>
<b>I.2</b>	<b>THE ADVENT OF TRUSTED COMPUTING .....</b>	<b>4</b>
<b>I.3</b>	<b>TRUSTED COMPUTING BY THE TRUSTED COMPUTING GROUP .....</b>	<b>5</b>
<b>II.</b>	<b>SOCIETAL, LEGAL, ECONOMIC AND TECHNOLOGICAL ASPECTS OF TC .....</b>	<b>6</b>
<b>II.1</b>	<b>SOCIETAL ASPECTS OF TC .....</b>	<b>6</b>
<b>II.2</b>	<b>ECONOMIC ASPECTS OF TC .....</b>	<b>8</b>
<b>II.3</b>	<b>LEGAL ASPECTS OF TC .....</b>	<b>9</b>
<b>II.4</b>	<b>TECHNOLOGICAL ASPECTS OF TC .....</b>	<b>11</b>
<b>II.5</b>	<b>OVERVIEW OF THE ASPECTS .....</b>	<b>12</b>
<b>III.</b>	<b>INITIAL FINDINGS .....</b>	<b>13</b>
<b>IV.</b>	<b>OPTIONS FOR THE WAY AHEAD .....</b>	<b>18</b>
	<b>ANNEXES .....</b>	<b>20</b>

## **O. Management summary**

Information and Communication Technologies (ICTs) are increasingly complex and pervasive in society and throughout the economy. Their uninterrupted, correct and secure functioning is critical for our well being and growth.

As new emerging ICTs, such as 'trusted computing' (TC), which administers and sometime restricts the functionality of a device to enhance its information security, have the potential to become even diffuse across all aspects of our life, an early understanding and anticipation of their possible societal and economic impacts would be desirable. For this reason, the European Commission has launched a debate on the potential public policy issues raised by the deployment of TC.

It is important to stress that a similar debate could be needed to analyse the impact of any technology that has the potential to progressively become vital to our life and economy. In general we need to ensure that technology would always be at the service of the users (private, business or public ones) as well as respect fundamental rights like the right to privacy, the freedom of choice and any other European democratic values which are so crucial for the development of an all inclusive, safe and respectful Information Society.

## I. Introduction

The purpose of the paper is to **raise awareness and launch a debate about the potential public policy impact of trusted computing (TC)**. This paper provides a short description of:

- trusted computing technologies (chapter I);
- potential impacts on society, economy, legislation, and technology (chapter II);
- some initial findings resulting from consultations with Member States (chapter III);
- options for action (chapter IV).

### I.1 Towards a secure Information Society

In its Communication "A Strategy for a Secure Information Society – Dialogue, Partnership and Empowerment"<sup>1</sup> the Commission recognised the urgent need to coordinate European efforts to develop policies, regulations, technology and awareness to build trust and confidence of businesses, public administrations and citizens in electronic communications and services. The Commission called for a "dynamic and integrated approach" to a secure Information Society that "involves all stakeholders and is based on **dialogue, partnership and empowerment**".<sup>2</sup>

Due to the increasingly complex nature of information and communication technology (ICT) and the societal need for them to be "trustworthy, secure and reliable"<sup>3</sup> as well as privacy-respectful, the opportunities and challenges of ICT in general and security technology in particular are more and more difficult to anticipate. Against this background, it is essential **to assess emerging technologies** and their public policy impacts especially from an interdisciplinary perspective that is "based on an open and inclusive multi-stakeholder dialogue"<sup>4</sup>.

Trusted computing is one such emerging technology. Essentially, it is intended to provide for secure data processing within a distributed and connected environment. In this respect, TC as a commercial off-the-shelf solution with hardware support **is intended to enable actors to better enforce their security policy** and help to govern their information assets that require up to a 'medium' level of security. Therefore, it can be considered as a means to simplify the management of security risks in such environments.<sup>5</sup>

---

<sup>1</sup> For more on COM (2006) 251 see [http://ec.europa.eu/information\\_society/policy/nis/strategy/index\\_en.htm](http://ec.europa.eu/information_society/policy/nis/strategy/index_en.htm) for information and [http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006\\_0251en01.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf) for download.

<sup>2</sup> See COM (2006) 251. Emphasis added.

<sup>3</sup> The Commission's initiative i2010, which was launched in 2005, states that: "Trustworthy, secure and reliable ICTs are crucial for a wide take up of converging digital services".

<sup>4</sup> See COM (2006) 251.

<sup>5</sup> To date, the European Commission (EC) funds several activities on TC – e.g. research projects ROBIN (<http://robin.tudos.org/>) and Open\_TC (<http://www.opentc.net/>) or call for a thematic network on trusted information infrastructures ([http://ec.europa.eu/information\\_society/activities/ict\\_psp/index\\_en.htm](http://ec.europa.eu/information_society/activities/ict_psp/index_en.htm)), etc.

## I.2 The advent of trusted computing

No single, commonly agreed definition of TC exists at present. This leaves room for improvement. In this paper, **TC** is understood **in a broad sense** as a set of hardware and software features embedded in the components of a computing architecture that supports the reinforcement of trust in computing. These so-called trusted components are platform<sup>6</sup>, operating system, middleware, application, and associated 'trusted' services.

However, it has to be stated clearly that the question of **terminology is not a trivial matter**. Terms such as confidence, trust, assurance, and security often overlap, provide for multiple interpretations and can prove difficult to define in their own right. In the following text therefore, the term 'trusted' means that a system "is relied upon to a specified extent to enforce a specified security policy"<sup>7</sup>. This more technical understanding of 'trusted' does however differ from the broader and more complex usage of 'trust' as a social construct.

**TC aims at supporting the provision of trusted services.** One possible example for such a trusted service could be online banking in the home environment. An example of a potential threat in a non-TC world is having a key logger installed on the personal computer (PC) without the user's knowledge. Such malicious programs are designed to 'capture' passwords when financial transactions are being processed. There is currently no way to counter this risk completely. Both the customer and the bank effectively operate on the basis that such capture is not happening until evidence to the contrary is forthcoming. In the future, however, it is hoped that with TC, online banking can be better protected so that transactions will only take place when the PC has not been tampered with by a malicious program and when it is confirmed that the PC that processes the financial transaction is the one it claims to be. With the help of TC, and specifically its hardware component, the customer and the bank can then exchange information with greater confidence that everything works fine. It is also anticipated that TC in combination with virtualization<sup>8</sup> will allow the running of online banking in a trusted environment while at the same time downloading software in an un-trusted environment – similar as having both things done in parallel on two separate PCs. In other words: TC would create a trusted environment based on a measured system state for the sake of security.<sup>9</sup>

The public policy relevance of trusted services will of course vary according to how these are deployed and who can put in force the respective security policies. Moreover, **whether a trusted service is considered as having a 'good'/ legitimate or 'bad'/ unjustified purpose might be difficult to decide** because security is a relative concept that depends on the intentions and perceptions<sup>10</sup> of the parties involved. Even if a decision can be reached, different parties involved in a service might also draw different

---

<sup>6</sup> According to [http://en.wikipedia.org/wiki/Platform\\_%28computing%29](http://en.wikipedia.org/wiki/Platform_%28computing%29) in computing, a platform describes some sort of hardware or software that facilitates the running of other software.

<sup>7</sup> According to [http://en.wikipedia.org/wiki/Trusted\\_system](http://en.wikipedia.org/wiki/Trusted_system) "[...] a trusted system is a system that is relied upon to a specified extent to enforce a specified security policy."

<sup>8</sup> According to <http://en.wikipedia.org/wiki/Virtualisation> "[...] virtualization is a broad term that refers to the abstraction of computer resources" and therefore hides the physical characteristics of computing resources from their users, be they applications, or end users.

<sup>9</sup> Besides online banking the EC funded research project Open\_TC also described virtual data centers and corporate computing on home PCs as application scenarios. More on this can be found here [http://www.opentc.net/images/otc\\_architecture\\_high\\_level\\_overview.pdf](http://www.opentc.net/images/otc_architecture_high_level_overview.pdf).

<sup>10</sup> For more on the psychology of security see <http://www.schneier.com/crypto-gram-0702a.html>.

conclusions from the behaviour of a trusted service. Therefore, a distinction between internal services run by organisations that only affect themselves and services that affect their customers (or the public at large) and/ or business partners might be needed.

### I.3 Trusted Computing by the Trusted Computing Group

Although, as discussed in the previous section, TC can be understood in a broad sense, the focus in this section lies on one particular initiative conducted by the Trusted Computing Group (TCG) which is an industry-led "not-for-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices"<sup>11</sup>. 'Trust' for the TCG means "the expectation that a device will behave in a particular manner for a specific purpose"<sup>12</sup>. The relatively **narrow meaning of TC** in this section is therefore understood to refer specifically to a particular family of technical specifications<sup>13</sup> issued by the Trusted Computing Group (TCG).<sup>14</sup>

At present, the TCG is the only industrial initiative that specifies the architecture for trusted components. Some trusted components such as the hardware component, have already been implemented. Others such as **applications and services** utilising this hardware component are beyond the scope of the TCG and **have not appeared in large scale yet**.

The core building block of the TCG's approach to TC is a hardware component, the so-called Trusted Platform Module (TPM). The TPM acts as a passive device that is triggered by other trusted components working together in a way that ensures measurement and reporting about the status of the computing platform. The various components allow for a trusted initialisation process of a computing platform: while the system is starting, the first component that runs checks the status of the second component, the second component checks the third component, and so on. This creates a chain of trust by expanding the trust that is rooted at least partially in the TPM over a trusted operating system to a trusted service. These trusted components altogether **provide reliable evidence of the system's state**. In some cases the evidence of the system's state is vouched for to a requesting service: this feature is called remote attestation<sup>15</sup>.

---

<sup>11</sup> See <https://www.trustedcomputinggroup.org/about/> with members such as AMD, Fujitsu Ltd., Hewlett-Packard, IBM, Infineon, Intel Corporation, Lenovo, Microsoft, Sun Microsystems, Seagate, Wave Systems.

<sup>12</sup> See ISO/IEC 11889-1/4 - Information technology - Trusted Platform Module.

<sup>13</sup> See <https://www.trustedcomputinggroup.org/specs/>.

<sup>14</sup> For a more precise description of the TC characteristics – as understood by the TCG – (1) memory curtaining, (2) secure input/ output, (3) sealed storage, and (4) remote attestation as well as pros and cons of TC, we refer to the literature:

[https://www.trustedcomputinggroup.org/groups/tpm/Trusted\\_Platform\\_Module\\_Summary\\_04292008.pdf](https://www.trustedcomputinggroup.org/groups/tpm/Trusted_Platform_Module_Summary_04292008.pdf);

[http://www.eff.org/Infrastructure/trusted\\_computing/](http://www.eff.org/Infrastructure/trusted_computing/);

[http://www.schneier.com/blog/archives/2005/08/trusted\\_computi.html](http://www.schneier.com/blog/archives/2005/08/trusted_computi.html);

<http://cyberlaw.stanford.edu/blog/stefan-bechtold>;

<http://www.cl.cam.ac.uk/~rja14/tpa-faq.html>.

<sup>15</sup> Attestation is the process of vouching for the accuracy of information. All forms of attestation require reliable evidence of the attesting entity. This can be achieved by shipping TPMs with an embedded key.

The **TCG specifications differentiate between 'owner' and 'user'**. The owner, who is similar to the administrator of a system, has control over the device but not always actual physical possession. Whereas in a corporate environment the administration is done by ICT professionals, in the private sphere an individual should be both owner and user. With regard to mobile phones, where the telecommunication operator instead of the subscriber has full control over the device, this might be considered as a significant issue for corporate as well as for individual users. Moreover, the balance of power between owner and user might be further altered to the benefit of the owner because of TC. TC could also provide more power to the manufacturers, developers or distributors of personal computing devices. By maintaining control over the TPM, they could force their customers into using specific solutions. Importantly, such a usage scenario could easily degrade the public perception of (and confidence in) TC. Therefore, it is expected that TC will get more complicated from a policy perspective when it leaves the enterprise realm and enters the world of consumers and citizens.

## II. Societal, legal, economic and technological aspects of TC

Security technologies are of course to be welcomed as measures to counter existing security risks. In addition, such technologies can boost new services. However, global and ubiquitous solutions for computing platforms and information systems may have **societal, economic, legal, and technological impacts beyond the actual technology** itself. In case of widespread deployment these impacts might be far reaching.

Our **analysis and discussion** with domain experts **identified the following general principles and basic requirements**. These principles and requirements have partially been debated and formed an input for the discussion with Member States.

### II.1 Societal aspects of TC

While welcoming the initiative of the private sector to "stimulate the deployment of security-enhancing products, processes and services", an **"appropriate societal balance between security and the protection of fundamental rights**, including privacy, is needed".<sup>16</sup> A means to contribute to this general principle is to empower individual users to understand and play their respective roles in the overall security chain. Sustainability<sup>17</sup> of information in the digital age – where and when necessary – is a key objective for technology deployment in the Information Society. Consequently, the basic requirements are **freedom of choice, user information and informational self-determination**<sup>18</sup> (see below).

**Freedom of choice: Technology must not undermine the freedom of choice.**

When users use computing platforms, they should decide, subject to certain constraints,

---

<sup>16</sup> See COM (2006) 251. Emphasis added.

<sup>17</sup> According to <http://en.wikipedia.org/wiki/Sustainability> "[...] the concept of sustainability [is] a fundamental, immutable value set that is best stated as 'parallel care and respect for the ecosystem and for the people within'. From this value set emerges the goal of sustainability: to achieve human and ecosystem longevity and well-being together. Seen in this way, the concept of sustainability is much more than environmental protection in another guise. It is a positive concept that has as much to do with achieving well-being for people and ecosystems as it has to do with reducing ecological stress or environmental impacts".

<sup>18</sup> See [http://en.wikipedia.org/wiki/Informational\\_self-determination](http://en.wikipedia.org/wiki/Informational_self-determination) for definition and [http://www.bundesverfassungsgericht.de/entscheidungen/rs20060302\\_2bvr209904.html](http://www.bundesverfassungsgericht.de/entscheidungen/rs20060302_2bvr209904.html) for ruling of the German Constitutional Court.

which software to execute and which data to access. They should control to some extent what their platform is doing and which other platforms it communicates with (including what data is exchanged). It is crucial that users *can consciously choose whether to use TC or not (controllability) while understanding what TC is doing (transparency)*. It is pivotal that, in case users have TC switched off or use non-TC technology, they *can access their data without restriction (accessibility)*. In some cases, however, a trusted service such as online banking that requests a defined system state might restrict the user's options to act for the sake of security. These requirements are true for both corporate and individual users.

**User information: Technology must be accompanied by understandable information about the technology and its implications.**

Although individual users play a role in the overall security chain, their responsibility has clear limits. The idea that all individual users will ever be informed enough to fully control their home environment is unrealistic. *Information asymmetries* are not expected to disappear by providing more information to the individual user but they *should nevertheless be minimised*. Individual users should be able to give informed consent to decisions proposed or even made by TC. If the needed information is publicly available, external experts could help individual users to reduce the information asymmetry. They could independently validate the security of TC, and improve public perception and trust.

**Informational self-determination: Technology must respect the right of an individual to decide what information about himself should be communicated to others and under what circumstances.**

To ensure authenticity and integrity of the computing platform, cryptographic keys and digital certificates are used as credentials. If an individual uses the same credential several times even in different contexts, there might be a risk to link the credential to the platform and thus to the individual user. If a credential contains more information than needed in a given context, there might be a risk that the communication partners gain more knowledge about the individual user than necessary or desirable. In both cases the *right to privacy and the protection of personal data should be maintained*.

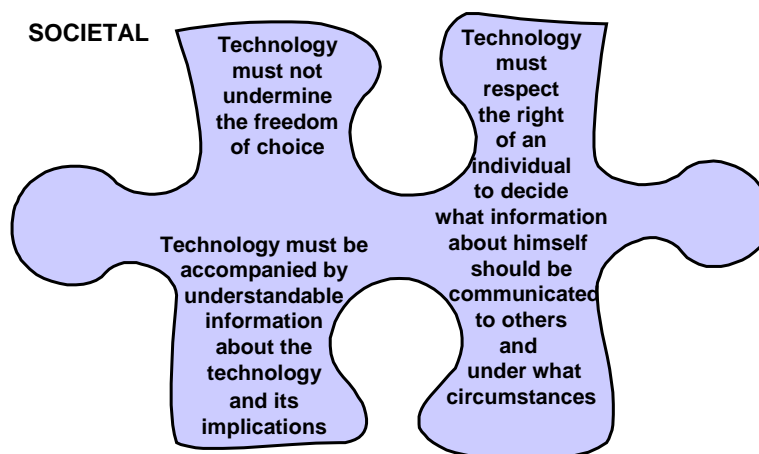


Figure 1: Basic societal requirements – freedom of choice, user information and informational self-determination

## II.2 Economic aspects of TC

The ICT industry in general and the security sector in particular play an important role in the European economy and are a major driver for growth in the EU. At the same time, there is a strong dependency of citizens, public administrations and businesses on ICT. "It is therefore of strategic importance that European **industry** be both a **demanding user** as well as a **competitive supplier** of network and information security products and services."<sup>19</sup> A means to contribute to this general principle is to appreciate security as an enabler of products and services as well as a potential competitive advantage for EU companies. Heterogeneity of technology and of technology suppliers is a key objective for technology deployment in Information Society. Consequently, the basic requirements are **fair competition** and **technological diversity** (see below).

**Fair competition: Technology must neither be exploited to achieve an abusive dominance of the market nor lead to increasing anti-competitive levels of concentration within the ICT industry.**

TC could be utilized to request a defined system state that is not completely justified by security considerations alone. The features of remote attestation might be misused to gain market control by locking-in users. The potential to cryptographically protect data could add to this risk because the user might not be in full control of the cryptographic means in order to access the data. Dominant actors might be tempted to enter into anticompetitive practices. Coupled to network effects<sup>20</sup>, this would pose a significant risk to *competition* and *innovation*. This then leads to reducing diversity and, by so

<sup>19</sup> See COM (2006) 251. Emphasis added.

<sup>20</sup> According to <http://www.economist.com/research/Economics/alphabetical.cfm?letter=N#networkeffect> network effect means that "[...] the value of a good to a consumer changes because the number of people using it changes".

doing, can generate negative security effects. Non-binding measures such as procurement recommendations for public administration that promote diversity and competition might therefore be seen as an instrument to counter this risk.

**Technological diversity: Technology must not act as a hindrance to the deployment of other technologies.**

All interested parties should be able to participate in the specification process and related reference implementations should be publicly available. The specifications should therefore be *open* and the specified interfaces should be *interoperable*. Openness and interoperability are prerequisites for the compatibility of TC. A lack of standardisation seems to be an issue, too. Consequently, small and medium sized enterprises or academic research institutes should neither be discriminated against by means of restricted membership conditions nor by unfair licensing fees. TC should not be utilized to *hamper other technologies* e.g. open source software<sup>21</sup>.

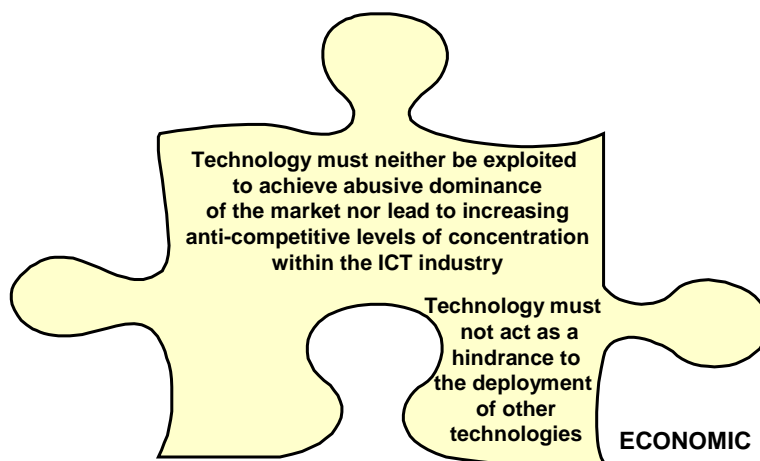


Figure 2: Basic economic requirements – fair competition and technological diversity

### II.3 Legal aspects of TC

The potential legal<sup>22</sup> drawbacks of a technology with possibly disruptive effects are very hard to anticipate and reiterate the need for us to "**recognise the respective roles of the various stakeholders**"<sup>23</sup>. A means to contribute to this general principle is that every stakeholder needs to recognise its own share in taking on responsibility. Auditability of what technology does is a key objective for its deployment in the

---

<sup>21</sup> According to <http://www.opensource.org/docs/osd> "Open source doesn't just mean access to the source code. The distribution terms of open-source software must comply with the [...]" open source definition. In practical terms, this means that Open Source Software must be distributed under a license that allows access to its source code, its modification and the redistribution of the program in its original or modified form, whether for free or for a fee.

<sup>22</sup> This aspect is the least mature one and needs further attention and examination.

<sup>23</sup> See COM (2006) 251. Emphasis added.

Information Society. Consequently, the basic requirements are **liability regimes** and **trust perception** (see below).

**Liability regimes: Technology must be supported by a framework that motivates the party best able to treat risks by internalising them.**

Ideally, the one who deploys a system should be the one who pays the costs when it fails, but it is often very difficult to identify responsibilities in a complex environment with various actors. Without clearly assigned responsibilities it is especially challenging therefore *to decide where liability lies and how to enforce it*. This is particularly important when discussing potential usage scenarios of TC and the distribution of power among the various actors involved (platform manufacturers, independent software and hardware vendors, operating system distributors, device owners, corporate and individual users, content and service providers). Whether TC, and more precisely trusted services that rely on the state of a system via remote attestation, will clarify the allocation of liability is an open question.

**Trust perception: Technology must be accompanied by an infrastructure that supports confidence building.**

Any statement related to trust needs to identify whom we are intending to trust and what for (a brand name, an organisation, a technical component). With TC, *control* over the user's information and platform *is delegated to some components of the TC architecture* and to the actor that enforces the respective security policy. The attested state of the system that is relied on by trusted services is based on cryptographic keys and digital certificates. These credentials are issued e.g. by a certification authority. Therefore, we primarily transfer power and thus trust to the technical component but secondarily also transfer power and thus trust to the organisations that issue certificates. Which rules and procedures they follow and how to establish confidence in this infrastructure is also an open question.

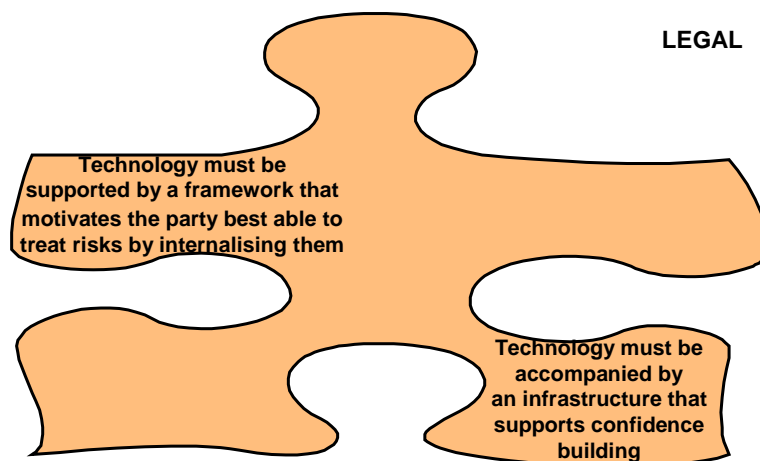


Figure 3: Basic legal requirements – liability regimes and trust perception

## II.4 Technological aspects of TC

"**Security is an asset in building trust and consumer confidence**".<sup>24</sup> A means to contribute to this general principle is to enhance the culture of security and give grounds for confidence that the technology does what it should (but does not do what it should not). Visibility of technical features including security/ privacy is a key objective for technology deployment in Information Society. Consequently, the basic requirements are **quality**<sup>25</sup> and **assurance**<sup>26</sup> (see below).

**Quality: Technology must neither put user data nor system availability at risk.**

There might be a risk that trusted components 'lock-in' users. *Portability* of user data is important in order to e.g. allow backups (itself an important element of security). There is also a risk of backward incompatibility of trusted components. *Maintainability* of systems is important, too, in order to e.g. install patches and updates/ upgrades or allow replacements. In addition, future developments in the field of cryptography and cryptanalysis should specifically be provisioned for. Besides technical feasibility, both requirements need to be accompanied by practical *usability*. TC should *not decrease the overall functionality including the overall level of security*; this is particularly indispensable for sensitive applications of critical business processes e.g. to replace a system in case of response to an incident.

**Assurance: Technology must not pretend unwarranted security features.**

In order to support the understanding of what trusted services that request remote attestation are doing, a set of properties that describe their behaviour is needed. If this is done properly, *auditing for compliance* against these properties is then possible. When a hardware component is used to establish the 'root' of trust chain, *security certification* would be useful to establish primary trust for this component. Evaluating against an appropriate level of assurance would also demonstrate that mechanisms are strong enough to resist attacks. In order to ensure the completeness and correctness of the implementation of trusted components, *testing for conformity* against publicly available specifications is needed. If those assessments are conducted by independent parties, this would add even more to the degree of assurance.

---

<sup>24</sup> See COM (2006) 251. Emphasis added.

<sup>25</sup> According to <http://www.cse.dcu.ie/essscope/sm2/9126ref.html> the objective of ISO 9126 "[...] is to provide a framework for the evaluation of software quality. ISO/IEC 9126 does not provide requirements for software, but it defines a quality model which is applicable to every kind of software. It defines six product quality characteristics and in an annex provides a suggestion of quality sub characteristics".

<sup>26</sup> According to <http://www.jtc1sc27.din.de/sce/SD6> assurance means "grounds for confidence that a deliverable meets its security objectives. This definition is adapted from ISO/IEC 15408-1:2005 and generally accepted within the security community; within ISO the more generally used definition is: Activity resulting in a statement giving confidence that a product, process or service fulfils specified requirements".

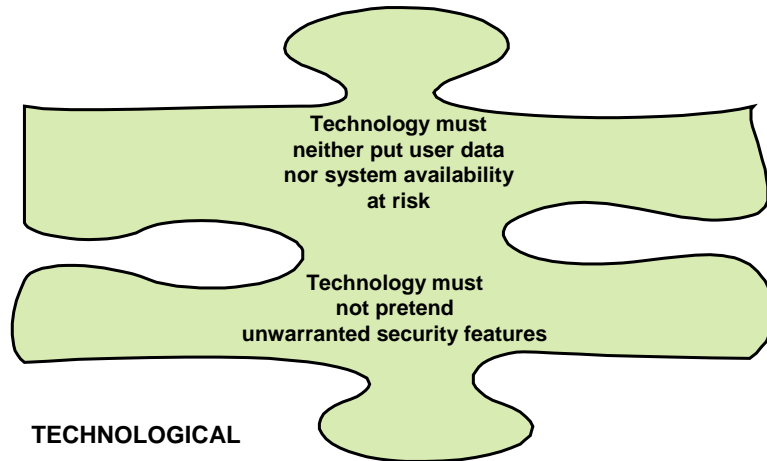


Figure 4: Basic technological requirements – functionality and assurance

## II.5 Overview of the aspects

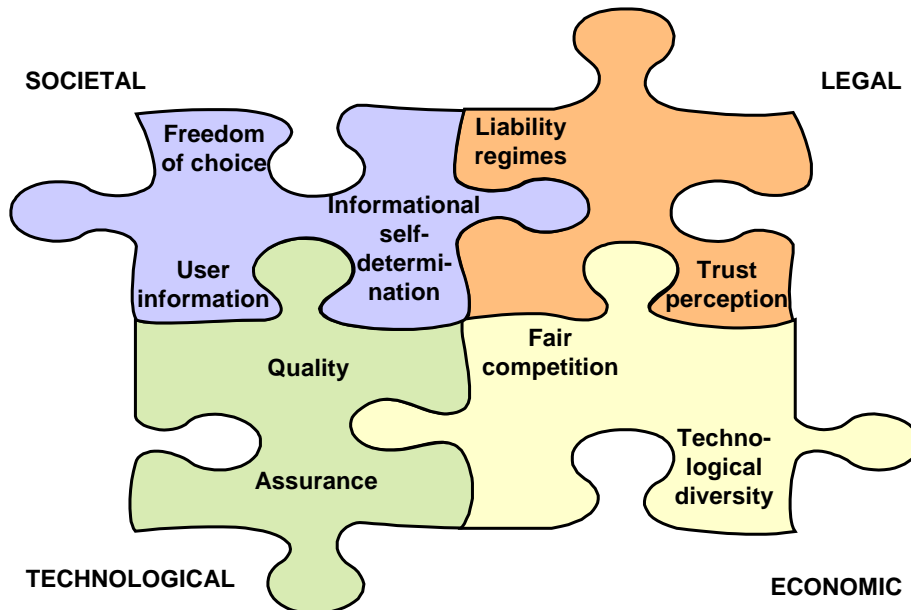


Figure 5: Overview of basic requirements with regard to societal, legal, economic and technological aspects of TC

Notwithstanding the potential of TC to contribute to information security, the extent to which TC might be effective in countering risks is not clear at the moment. The role of TC for the future of the Information Society therefore needs to be clarified e.g. by **debating desirable and non-desirable usage scenarios of TC** within an open and inclusive multi-stakeholder dialogue.

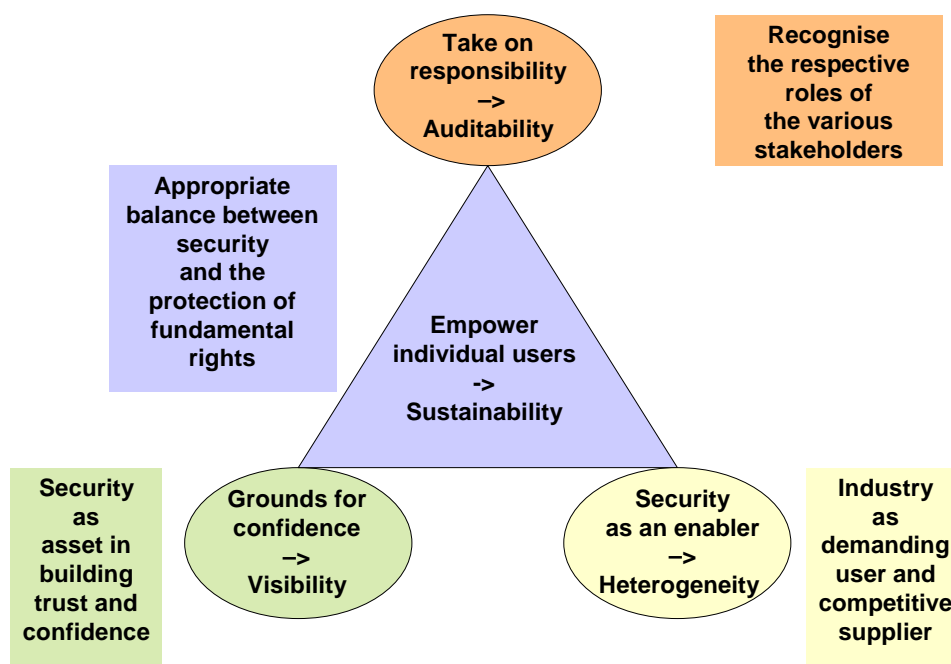


Figure 6: Overview of general principles, means and key objectives

### III. Initial findings

The general principles and basic requirements mentioned in the previous chapter were instrumental **to launch and stimulate a discussion** with Member States on trusted computing<sup>27</sup> (see Annex D)<sup>28</sup>. Speakers from four Member States (Germany, United Kingdom, France, and Austria) presented their views and experiences on the key issues to each other and to participants from other Member States (Ireland, Hungary, Malta, The Netherlands, and Norway).

Computing platforms are already been shipped with TPMs inside<sup>29</sup> but only a few applications currently use the TPM<sup>30</sup>. An application that is 'suddenly' rolled out might however, induce **large scale deployment, effectively 'over night'**. Therefore, public policy impacts need to be discussed while there is still time to influence the development and the deployment of TC. Once applications are out, issues such as key management, organisational integration, and operational complexity will need to be tackled by organisations that deploy TC anyway.

When it comes to public policy impacts, **TC clearly has a European dimension:**

<sup>27</sup> The actual discussion and therefore the rest of this section are mainly addressing the TCG's approach to TC.

<sup>28</sup> The opinions expressed in such workshops are by nature not official positions.

<sup>29</sup> The study "Industriepolitische Auswirkungen von sicheren IT-Plattformen auf Basis der 'Trusted Computing' (TC) Technologie – Projekt Nr. 46/07" postulates an area-wide coverage by 2015; see p. 26 of [http://www.wik.org/content/trusted%20computing\\_2008\\_07\\_28.pdf](http://www.wik.org/content/trusted%20computing_2008_07_28.pdf).

<sup>30</sup> An example of an application that currently uses the TPM is hard disk encryption in order to avoid data disclosure in case of device theft. An envisaged application could be to use the TPM to improve the security of systems isolating classified/ unclassified data. Others could be for mobile phones or network admission control - however, platform authentication should be kept separate from personal authentication. A TPM might be used, too, to enforce privacy-respectful data processing by third parties in order to improve identity management.

- European values such as freedom of choice and privacy should not be traded-off when delegating control to a technical component;
- technological diversity comprising interoperability and openness is the prerequisite for competition and innovation;
- European industry and in particular small and medium sized enterprises as well as open source software producers have asked for a level playing field encompassing all actors.

The timeline as well as means and partners for possible actions become clearer by mapping the aforementioned policy issues to the questions: (i) How specific to TC are the issues? (ii) In which component of the computing architecture do the issues manifest themselves? **The deployment of trusted platforms takes place at present – the development of trusted services will appear later.** However, it might be oversimplifying to consider some issues as short-term and others as long-term targets.

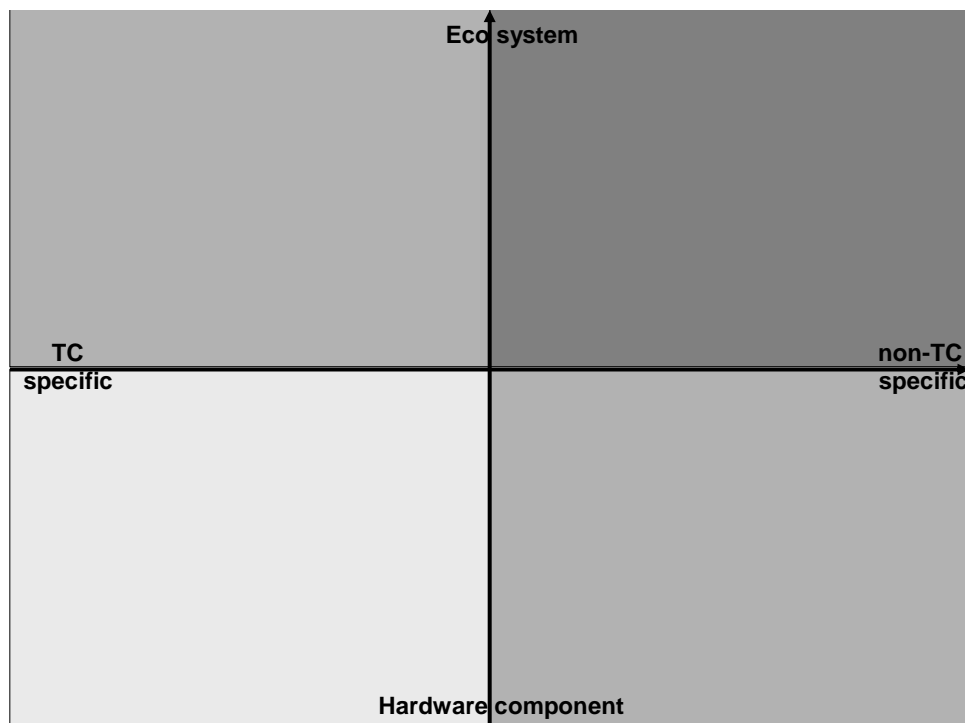


Figure 7: Questions of TC specificity and vertical integration

The points made in the debate were mainly **issues related to assurance** which is one of the **technological aspects** mentioned in chapter II.4.

The **TPM** is a passive device that could support the enforcement of the security policy required by an application. Its presence could be invisible to users and its security functionality could be **considered as a commodity of the platform and application**. Nevertheless, trust in a TPM requires scrutinising the provided security functionality. Regarding assurance, there are three issues that currently pose concerns:

- Only 1 out of the 11 companies that form the TCG board of directors is a European based company. Allowing for the dependency on ICT in general, the EU relies on non-European equipment manufacturers in particular. On top of this, the EU might be faced with **TPMs that are not fully conformant to the TCG specification** that was recently approved as ISO/IEC 11889.

- The **TPM** should be evaluated against Common Criteria<sup>31</sup>. More specifically, the TPM should be **certified** the same as smart cards are. Whether only discrete TPMs can achieve this level or TPMs integrated into the CPU as well is an open question. The TCG has drafted a protection profile<sup>32</sup> **targeting EAL4+**<sup>33</sup>. But whether technology providers will deliver certified TPMs and technology users will procure certified TPMs is an open question.
- Moreover, it is worth saying that trusting a TPM is not enough to establish trust for a platform. Trust in other components of the platform and beyond are also needed. Any application that uses a TPM should state that the security functionality is justified as much as that the application's behaviour is transparent. Criteria, methodology and parties have not yet been discussed. To find **simple but meaningful behavioural properties to attest in order to transparently demonstrate what the application is doing** seems to be quite a challenge. The TCG has already discouraged coercion by vendors and laid out principles underlying the design of TCG specifications in a best practice principle document<sup>34</sup>. But whether these principles have sufficient granularity to allow auditing for adequate compliance is – like other issues related to remote attestation – an open question, too.

Assessments conducted by independent parties would not only increase the visibility of security but also give additional grounds for confidence in the secure functioning of ICT – which shows a path 'to go from security to trust'. **TC and particularly the TPM as the root of trust need more than 'blind faith' to be trusted.**

The three issues related to assurance are particularly important in **critical information infrastructures and sensitive governmental applications**, where undocumented, hidden or crippled functionality as well as an inability to replace a system in case of recovery from a disaster are not acceptable.

In addition to issues related to assurance, **interoperability, transparency and freedom of choice** were points made in the ongoing debate. Neither these requirements nor others mentioned in chapter II.4 have been discussed.

---

<sup>31</sup> Standardised as ISO/IEC 15408; see also [http://en.wikipedia.org/wiki/Common\\_criteria](http://en.wikipedia.org/wiki/Common_criteria).

<sup>32</sup> According to [http://en.wikipedia.org/wiki/Protection\\_profile](http://en.wikipedia.org/wiki/Protection_profile) a protection profile is a document used in the evaluation against the Common Criteria.

<sup>33</sup> The evaluation assurance level is augmented for resisting moderate attack potential; for details see chapter 6.2.3 of <http://www.bsi.de/zertifiz/zert/reporte/pp0030b.pdf>.

<sup>34</sup> See "Design, Implementation, and Usage Principles", Version 2.0, December 2005 via [https://www.trustedcomputinggroup.org/specs/bestpractices/Best\\_Practices\\_Principles\\_Document\\_V2\\_0.pdf](https://www.trustedcomputinggroup.org/specs/bestpractices/Best_Practices_Principles_Document_V2_0.pdf).

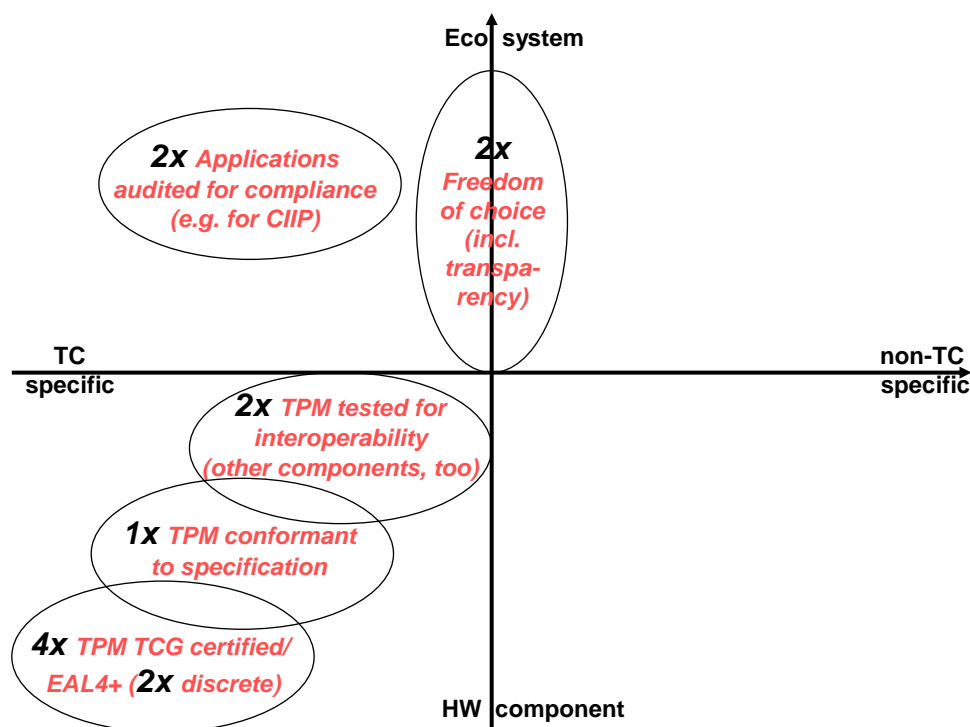


Figure 8: Similar needs expressed by speakers and supported by participants – whereas 1x means that 1 out of 4 speakers mentioned a particular issue etc.

With regard to assurance, there was one issue mentioned but not elaborated at the workshop – **the Chinese approach towards TC** – and this boxed text should serve as additional information for the interested reader:

In the context of **TC**, China has issued specifications with regard to the hardware component and its interface with the central processing unit (CPU). These specifications seem to have not been developed openly and are only partly publicly available. The Trusted Cryptography Module<sup>35</sup> (TCM), the Chinese variant of the Trusted Platform Module (TPM), is allegedly based on TPM version 1.2 but not fully conformant. **Cryptographic algorithms and the communication protocols between TCM and CPU were reported to be subject to changes.**

This information demands further substantiation in the light of possible concerns regarding hampered **interoperability** between TC technologies **as well as** limited **compatibility** between applications or services that are enabled by TC technology. This might also lead to restricted **inter-connectivity** at a global level.

In the case of **home-grown cryptography required for domestic usage**, this might mean that cryptography **could be weaker because of proprietary algorithms or obscure features**. Cryptography that is easier to break or circumvent might be intentionally used by countries enforcing privacy not compatible with EU principles and legislation in order to e.g. conduct industrial espionage. This might cause new trade barriers, too

Undoubtedly, governments and public administrations have a key role to play. In this context, public procurement needs to fulfil the role of 'demanding technology user' or 'likely TC adopter'. Understanding the technology and its impacts as well as communicating governmental views to industry is a powerful tool for being provided with the technology wanted. The bigger the market, the more likely industry will supply

<sup>35</sup> See [http://www.zteic.com/en/news\\_details.aspx?id=244](http://www.zteic.com/en/news_details.aspx?id=244).

the technology that fits the needs of Member States. The market of one Member State alone however, is almost certainly too small. Harmonising procurement within Member States is however a known challenge, let alone aligning procurement across borders. Due to limited resources within Member States it is difficult for Member States to investigate TC, let alone to express their needs. If governments and public administrations do not want to be obliged to take what industry offers, **better coordination and cooperation within and among Member States could lead to a better understanding of the technologies and create sufficient market demand to shape the supply-side.**

**Initial analysis suggests that TC is an emerging technology that:**

- is anticipated to solve some of the 'old' information security challenges but not to serve as a panacea to all possible problems such as spam, malware, phishing, etc.;
- is sometimes perceived to facilitate (and possibly aggravate) anti-competitive behaviour;
- is seen to also create 'new' information security challenges both from an ICT perspective and in terms of social and legal issues.

For any emerging technology, experience suggests that the focus of public policy should be on the **framework conditions for development and deployment of the technology**. Actual trends of TC such as the amount of shipped TPMs or the need for assurance have to be taken into account to help focus on the 'right' framework conditions. The nature of efforts to create such a framework with regard to TC will vary with the view we have on TC. A debate is required on about:

- whether and where TC will be desirable (or not) as well as
- what will be an acceptable trade-off in certain usage scenarios of TC.

Understanding the public policy impacts of TC as a dynamic and complex technology needs to be based on an interdisciplinary debate involving all stakeholders. **The strong interdependency between technology and Information Society calls for a more proactive, innovative and flexible approach.** In this context, the following preliminary conclusions on TC would help to identify possible options for action.

- The small number of registrations for the workshop – only 9 Member States – shows that awareness still needs to be raised in Member States before more representative conclusions can be made. Nevertheless, the concept of the workshop was seen as an efficient way of **being aware of the dynamic and complex technology and its potentially important policy impacts**. In addition to that, there is an apparent need **to exchange views between early adopters and those pursuing a slower approach as well as share experiences already gained**.
- The presentations in combination with the discussion indicated that there is common ground for the development of basic requirements (such as security certification) as well as general principles (such as freedom of choice). The to-be developed requirements and principles could support governments and public administrations so as **to help them procure the technology that maps**

**their needs and to guide the deployment of the technology to fit good administrative practices.**

By acknowledging the fact that the issue is a similar one in many emerging technologies, the most consistent option at EU-level would be not to address each and every technology separately, but to take a **more holistic and technology-neutral** (not technology-ignorant) **approach** in looking for creative ways **to address the challenges on the Information Society in a pragmatic, result-oriented manner.**

#### **IV. Options for the way ahead**

Further to the analysis of the initial findings and the discussion with Member States some options for action are identified with a view to:

- raise awareness, exchange views and share experiences;
- develop a commonly agreed understanding of the issues at stake and better support Member States;
- better understand the economics of security and privacy.

Specific actions in the context of TC may ideally be complemented by a **policy forum for emerging technologies**. Such a policy forum could provide a neutral and objective platform for strengthening and supporting a wider public debate about the future role of technology in Information Society.

##### **Option 1: High-level conference on trusted computing**

- High-level conference towards the end of 2009 or beginning of 2010 under the auspices of the Council Presidency bringing together Member States and industry in order to **develop a common understanding of the major public policy impacts of TC**.

In preparation of the high-level conference, the following events may be organised:

- Follow-up workshop with Member States in the first half of 2009 for **raising awareness** as well as **exchanging views and sharing experiences** in order to continue the discussion on basic requirements and general principles;
- Seminar with Member States and other relevant stakeholders in the second half of 2009 in order to further discuss how **basic requirements** could be translated into a **template for public procurement of technology** and how **general principles** could be translated into **guidance on technology deployment**.

##### **Option 2: Study on the economics of security and privacy**

Further investigation of the economics of security and privacy is needed in order to investigate **competition, responsibility, and trust issues**. The study could focus on market forces, incentive structures, competition policy and lessons learnt from economic theory in order to analyse their relationship with the development and deployment of technology. Content-wise, **the study would concentrate on different technologies and various sectors** by conducting a case-by-case analysis. Remote attestation feature as well as the mobile phone usage scenario could be envisaged. This could help not only to deal with a single technology but to generalize from concrete instances to overall statements. The findings and recommendations of the study would

be discussed publicly – which will eventually be followed by a broader public consultation.

## Annexes

### A **Workshop with experts on 15 January 2007**<sup>36</sup>

One element in this reflection process was an expert workshop on "Public policy issues related to trusted computing". The morning was dedicated to participants' statements on potential public policy impacts related to trusted computing and the afternoon was spent to discuss crucial issues to be dealt with at EU level.

### B **Workshop under the German Presidency**<sup>37</sup>

The Federal Office for Information Security (BSI) held a workshop on "Trusted computing from a European Perspective – The impact on the public sector" within the framework of the German EU Council Presidency to discuss the impact on public authorities in Europe and their possible influence on trusted computing. The event took place at the Science Centre in Bonn on 26 and 27 February 2007. Approximately 70 IT and administration experts participated to discuss the opportunities and risks involved in the use of trustworthy information technology in a public environment.

### C **German Federal Government position paper**<sup>38</sup>

The key requirements on "Trusted Computing" in an updated "key issues" paper that takes into account the latest technological developments – produced by the German government – has laid out what its needs and requirements are with respect to Trusted Computing technology. Representatives from the German Interior and Economics Ministries have introduced this paper into the work of the Trusted Computing Group.

### D **Workshop with Member States on 28 May 2008**<sup>39</sup>

Another element in this reflection process was a workshop that raised awareness and highlighted issues related to trusted computing from a public policy perspective. Speakers from the public and the private sector addressed Member States officials and experts involved in policy making.

The purpose of the workshop was to bring together representatives from Member States in order to raise awareness about potential long-term prospects and impacts that might be of interest to policy makers, to provide a platform for identifying relevant public policy issues that deserve closer monitoring, and to discuss the way forward and possible actions at European level.

The workshop was structured in two parts: An open morning session with presentations illustrating the bigger picture and underlining impacts beyond technology. And a closed afternoon session with Members States presenting their views and experiences as well as discussing open issues and preferred ways to deal with them.

---

<sup>36</sup> For more information see [http://ec.europa.eu/information\\_society/policies/nis/docs/TC/Report150107.pdf](http://ec.europa.eu/information_society/policies/nis/docs/TC/Report150107.pdf).

<sup>37</sup> More on this can be found here [http://www.enisa.europa.eu/doc/pdf/publications/enisa\\_quarterly\\_09\\_07.pdf](http://www.enisa.europa.eu/doc/pdf/publications/enisa_quarterly_09_07.pdf) (pages 12-13 in ENISA Quarterly, Vol. 3, No. 3, Jul-Sep 2007).

<sup>38</sup> More on this can be found here <http://www.bmwi.de/English/Navigation/Technology-policy/The-information-society/secure-it-platforms.did=241614.html>.

<sup>39</sup> For more information see [http://ec.europa.eu/information\\_society/policy/nis/strategy/policies/trust\\_computing/slides/index\\_en.htm](http://ec.europa.eu/information_society/policy/nis/strategy/policies/trust_computing/slides/index_en.htm).

## **E Non-exhaustive list of questions to be explored further<sup>40</sup>**

### **Questions worth addressing are:**

- "Who should have ultimate control over the security policy of a trusted computer, and how can we place effective limits on this control?"<sup>41</sup>
- What is 'the added value of TC for security' and what are 'the ingredients that make TC trustworthy'?
- When TC aims at facilitating risk management while data is processed, 'whose risk are we talking about' and 'who finally controls the data'?
- The question 'what public interest is at stake with and without TC' cannot easily be answered.
- ...

### **Questions associated to the societal aspects and that may lead to further discussion are:**

- Who decides which security policy is enforced and when?
- How can one be reassured that such a security policy respects the interests of all the parties involved?
- How can the behaviour of a TC-enabled service be disclosed to the end user and what are the minimal requirements that need to be stated?
- Which other building blocks are involved in implementing the alternative privacy-friendly protocol (Direct Anonymous Attestation - DAA) and who decides to use it?
- Which data will need to be communicated to the service requesting the attestation (challenger) and what (property) evidence about the platform is really needed?
- How to strike the right balance between security needs and the protection of fundamental rights?
- How to ensure auditability?
- ...

### **Questions associated to the economic aspects and that may lead to further discussion are:**

- What can public policy makers do to minimise the risk that a dominant market player will not abuse the deployment of TC for anti-competitive reasons?
- What could be done to further ensure/promote appropriate conditions for a competitive European industry?
- Which components of the whole TC architecture should be regarded as crucial in order to ensure real competitiveness?
- Which purposes of TC-enabled services are detrimental for competitiveness and innovation?
- How can competition and innovation be ensured?
- What is needed to secure a competitive position of EU industry?
- ...

### **Questions associated to the legal aspects and that may lead to further discussion are:**

- Who should be the certification authorities involved in issuing TC-related certificates and who should be the validation entities?

---

<sup>40</sup> To be revisited later.

<sup>41</sup> See p. 3 of <http://www.cs.auckland.ac.nz/~cthombor/Pubs/itg06gtc.pdf>.

- Will a delegation of trust to the machine lead to more or less responsibility or liability of device manufactures and service providers and what does this mean for the whole TC architecture or its supporting trust infrastructure?
- Could remote attestation lead to non-repudiation of the transaction and is the user of a TC-enabled platform still responsible for what's happening on the machine when running a TC-enabled service on it?
- Which intellectual property rights issues need to be considered in the context of TC?
- What are the legal issues of the surrounding trust infrastructure?
- Is the existing anti-trust legislation sufficient?
- ...

**Questions associated to the technical aspects and that may lead to further discussion are:**

- How can an end user recognise TC-enabled platforms and services that misuse TC for other than security purposes?
- What could be done in order to distinguish between services using TC for good or bad purposes?
- What could be done in order to distinguish between genuine and obscure chip implementations?
- How can trust and confidence be increased with TC?
- Which open standards and interoperable interfaces are needed?