Trusted Computing Group

Design, Implementation, and Usage Principles
Version 2.0[1]

Authorship: TCG Best Practices Committee[1]

December 2005

[1] Supersedes 'TCG Design Implementation and Usage Principles for TPM-Based Platforms' Version 1.0

TCG is an industry standards body formed to develop, define, and promote open specifications for trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices. TCG specifications are designed to enable more secure computing environments without compromising functional integrity and with the primary goal of helping users to protect their information assets from compromise due to external software attack. Every effort has been made to write TCG specifications such that only a clear and single interpretation is possible. TCG will update its specifications if ambiguities are discovered.

More information and the organization's specifications are available at the Trusted Computing Group's Web site, www.trustedcomputinggroup.org.

Contents

Purpose and Audience

The Trusted Computing Group (TCG) has set for itself the ambitious goals of improving the security of the platform and infrastructure while:

i. preserving privacy, backward compatibility, and owner control

ii. promoting ease-of-use

iii. designing the technology so that it is interoperable

iv. ensuring that the user's data, while secure and protected, remains portable and accessible as needed in alternative modalities

This document lays out the principles underlying the design of the TCG specifications. Many of these principles are already inherent in the TCG specifications. TCG believes that an explicit statement of these principles will help guide the implementation and use of TCG-enabled components and their incorporation in larger systems and services.

Although there are inherent limitations that a specification setting organization has with respect to enforcement,[2] the provision of a design rationale and “application notes” is a well-established practice for component designers. There are design features in the TCG specifications that directly support the principles detailed in this document. These features favor a principled usage of the technology. Explaining their intended use makes the specifications more comprehensible and more likely to be used appropriately. However, while TCG can develop and publish positively biased technical specifications for component devices, it can only offer guidance and encouragement for those designing solutions incorporating them. Enforcement, if necessary, will be done by other organizations.

Many companies will have a strong self-interest in following best practices. They will want to be seen as responsible corporate citizens and will want to comply with “best practices” behavior. TCG expects that public review, or perhaps independent auditors will check whether companies comply with the TCG best practices. These best practices may also be considered by government and regulatory agencies in pursuit of their responsibilities to the public at large.

TCG intends that these principles be comprehensible not only to TCG members but also to those who will be affected by the deployment of TCG technology. TCG has therefore written this document to be readable by those without a background in computer security or specific knowledge of the TCG concepts and terminology. An

[2] TCG does not own or license any patents or other intellectual property necessary to implement these specifications. These Design, Implementation, and Usage Principles for TPM-Based Platforms are offered as guidance rather than as legally binding terms of use. Moreover, TCG cannot be responsible for the manner in which individual companies or others implement the TCG specifications in products or other services.

exception to this is the use of the TCG-specific definitions of “owner” and “user.” Although today implementers typically assume that the user of a machine is the platform owner, TCG terminology separates these two roles. The TCG specifications use “owner” to mean the owner of the system whose policy is being implemented with the aid of TCG-enabled capabilities, while “user” denotes the individual who is currently making use of the system. This is similar to the difference between the administrator and a user of a system; note that the owner cannot access the users’ private keys or data protected with these keys. It is important that readers of this document be aware of the distinction between owner and user.

In the corporate setting, it is typical that the platform owner is the corporation, with technical expertise provided by a group of Information Technology (IT) specialists, while the user is a particular employee. In the case of the home user, both roles are usually filled by the same person. Such an owner-user in this situation typically has less technical expertise than an IT department and thus is likely to find it more difficult to implement fine-grained control over TCG functionality. This issue is covered in more depth in the interoperability, controllability, and ease-of-use sections.

Introduction to the Principles

The principles that TCG believes underlie the effective, useful, and acceptable design, implementation, and use of TCG technologies are the following:

- **Security:** TCG-enabled components should achieve controlled access to designated critical secured data and should reliably measure and report the system’s security properties. The reporting mechanism should be fully under the owner's control.

- **Privacy:** TCG-enabled components should be designed and implemented with privacy in mind and adhere to the letter and spirit of all relevant guidelines, laws, and regulations. This includes, but is not limited to, the OECD Guidelines,[3] the Fair Information Practices,[4] and the European Union Data Protection Directive (95/46/EC).[5]

- **Interoperability:** Implementations and deployments of TCG specifications should facilitate interoperability. Furthermore, implementations and deployments of TCG specifications should not introduce any new interoperability obstacles that are not for the purpose of security.

- **Portability of data**: Deployment should support established principles and practices of data ownership.[6]

---

[3] http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html
[4] http://www3.ftc.gov/reports/privacy3/fairinfo.html
[5] http://www.europa.eu.int/comm/internal_market/privacy/law_en.htm
[6] Note that these vary by geography.

- **Controllability**: Each owner should have effective choice and control over the use and operation of the TCG-enabled capabilities that belong to them; their participation must be opt-in. Subsequently, any user should be able to reliably disable the TCG functionality in a way that does not violate the owner's policy.

- **Ease-of-use**: The nontechnical user should find the TCG-enabled capabilities comprehensible and usable.

As with any worthwhile set of principles, each one in isolation is desirable; the challenge is to appropriately manage the potential conflicts between them. In some cases, these discordances can be resolved at the expense of some other desirable attribute (for example, simplicity or economy). In other cases, conflict is inevitable. Sometimes the TCG specification developers have chosen a particular balance between conflicting goals. On other occasions, the TCG design provides flexibility that allows — indeed, requires — the balance to be struck by those who make use of the TCG-enabled capabilities. Fortunately, often principles that seem in conflict may actually support and complement each other. For instance, effective security is essential if any data (private, corporate, etc) is to be protected.

TCG anticipates the development of infrastructure to support the privacy functionality designed into the TCG-enabled capabilities such as the Trusted Platform Module (TPM). To be effective at providing the privacy protections anticipated by TCG, this infrastructure must be easy to understand and use. The privacy services provided must also be available at an end-user cost that is acceptable. Furthermore, attestation (an assertion of the TCG-assured data about the system configuration) of the security properties of a platform should not be used to interfere with interoperability; developers of infrastructures should require attestation only for such operations where security provided by attestation is necessary for security.

Implementations of TCG technology, like many security and privacy technologies, are subject to applicable laws and regulations.

Security Principle

TCG-enabled components should achieve controlled access to designated critical protection of secured data and should reliably measure and report a system's security properties. The reporting mechanism should be fully under the platform owner's control.

Strong support for the platform owner's security policy is the primary goal of the TCG. The security principle is intended to remind implementers, solution designers, and users that the mechanisms in themselves provide only a foundation for achieving platform security. TCG technology will not thwart all attacks and should be only one aspect of a "defense-in-depth" strategy.

Good security requires attention to all aspects of the system, including personnel, procedures, and physical security. Software components that deal with authorization values, which are used extensively to establish authorization to use a protected

resource, should guard the values and any passwords they are derived from to an appropriate standard of care. Similarly, organizations using cryptographic signatures as part of a TCG-related deployment, such as issuers of platform security credentials, should exercise appropriate custody over the private keys used to form such signatures.

Privacy Principle

TCG-enabled components should be designed and implemented with privacy in mind and adhere to the letter and spirit of all relevant guidelines, laws, and regulations. This includes, but is not limited to, the OECD Guidelines, the Fair Information Practices, and the European Union Data Protection (95/46/EC).

The above-mentioned guidelines can be applied to TCG-enabled solutions as follows:

- Notice: Explicit notice of the collection and retention of personal data should be provided.

- Choice: The owner of TCG-enabled capabilities should have effective choice and control over the transfer of personal information. Users of TCG-enabled capabilities should be able to reliably disable the TCG capability in a way that does not violate the owner's policy but that allows the user to have control over the transfer of personal information.

- Purpose Limitation: Personal information collected for one purpose should not be used for another. **All implementations of TCG-enabled components should ensure that the TCG technology is not inappropriately used for data aggregation of personal information.**

- Control: Private information about the owner should be under the platform owner's control. Private information about the user should be under the user's control.

- Data Quality: Any stored information should be disposed of in a timely fashion and, as a consequence, any personal information supplied as a result of TCG-enabled technology should be up-to-date.

- Access: If TCG-enabled capabilities are used in collecting or storing personal data about an individual, there must be a way for the individual to review and correct such data as needed.

- Proportionality: Personal data that is collected and transferred through TCG-enabled capabilities must be both relevant and not excessive with respect to the purposes for which it is collected. Private keys, which play fundamental roles in protecting privacy on the platform, should *never* be disclosed.

Proportionality is part of the fundamental security model of the TCG specifications. For example, the TPM incorporates a single long-term stable identifier called the platform's Endorsement Key (EK). Since the TPM is bound to the platform, the EK becomes personally identifiable information. In order to reduce the capability for aggregation of personal data, the TCG specifications specifically forbid the general use of the EK. Instead, these require that the EK be used to generate aliases that should not be linkable back to an explicit EK. This can be done in a variety of ways including the use of zero-knowledge protocols, through a Privacy Certification Authority (CA), through a combination of zero-knowledge protocols and a Privacy CA, etc. Use of such tools protects the user's privacy by making data aggregation much more difficult. TCG recommends that implementations and deployments of TCG-enabled systems enable the highest degree of anonymity appropriate for a given situation.

Interoperability Principle

Implementations and deployments of TCG specifications should facilitate interoperability. Furthermore, implementations and deployments of TCG specifications should not introduce interoperability obstacles.

Interoperability is a challenge for all new technologies and standards - TCG is no exception. TCG technologies will not eliminate interoperability problems but neither should TCG technology make interoperability issues worse. Using TCG technology to create barriers to interoperability would violate the Interoperability principle and the TCG best practices. For example, service providers should not require users to have TCG-enabled technologies in order to obtain service unless the service requires such a level of security.

The more tightly focused application of this top-level principle is directed toward implementations of components directly specified by TCG specifications.

- TCG specification-defined APIs (core and optional) should be adhered to without modification.

- TCG specification-defined protocols (core and optional) should be adhered to without modification.

- TCG specification-defined data formats (for example, for cryptographic certificates) should be adhered to without modification.

These principles are essentially statements of what it means to be a "standard" and the behavior expected of bodies that claim to implement components according to a standard. Their aim is to foster interoperability. This would enable a realistic market

between components claiming conformance to the TCG specifications while avoiding confining buyers of TCG technology to a single supplier or narrow group of suppliers.

By contrast, the further-reaching principles below concern neutrality and open access among suppliers of solutions making use of TCG-enabled components:

- Applications using TCG-enabled capabilities to determine system configuration should base their decision to interoperate on the conformance of the measured configuration only for the purpose of clearly-disclosed and publicly-available security goals.

- Solution designers are encouraged to use and create technical and market mechanisms for open, objective certification of relevant properties of TCG-measured components.[7]

Portability of Data Principle

Deployment should support established principles and practices of data ownership.

The TCG-enabled technology uses encryption keys to protect the user's data. For TPM-based platforms, what is unusual about the TCG environment is the sealed hardware protection of certain encryption keys. There are two types of hardware protections: “protected storage” and “sealed storage.” Following standard data-protection models, protected storage means that encryption keys and data protected by those keys are under controls enforced by the TPM. In sealed storage, an additional capability has been added, namely the requirement that the protected information, whether keys or data, can only be revealed when the device is in a particular software state. This powerful facility has many benefits; it supports the Security and Privacy principles, for example, and can deliver important protections. However, without appropriate safeguards, sealed storage also has the potential to undermine the portability of the data so protected.

Data portability has been a central concern in the development of TCG technologies. An example of support for data portability in the TCG specifications is the provision for “migratable” keys. Keys that are used to protect application data may be marked “migratable” to facilitate backup and transfer to other environments (whether or not those are TCG-enabled). Provision is also made for recovery of TPM-protected data where either the original TPM is no longer functional or the system in which it was embedded has broken down. This part of the specifications is more complex, requiring the principle of data portability to be balanced against the principle of

[7] An example of adherence to this principle within the TCG specifications is the deliberate absence of a single “TCG root” (either in the form of a cryptographic key or an organization) which would be responsible for itself certifying conformance to TCG criteria. Instead, the specifications foresee self-certification of conformance by component manufacturers, possibly backed by independent certification organizations. The acceptability of any certifications to the bodies that produce platform aliases on demand, and the acceptability of those bodies to particular application environments, is a matter deliberately left to those bodies and their clients.

security (the resolution of the conflict is at the expense of ease-of-use). Where supported, data migration should be simple and straightforward; implementers should ensure that unsophisticated users will be able to migrate data efficiently (when they are permitted to do so by the platform owner).

The following portability principles should be applied:

- Any application that uses TCG technology to bind data to the platform or application should either:

    a) provide a means to export that data from the TCG security envelope, or

    b) provide appropriate, effective, and timely notice to anyone with a reasonable expectation of access to that data of the absence of data export and the consequences of such an absence.

- TPM-protected keys should be designated as "nonmigratable" only where there is a clear security requirement for nonmigratability.

- While for security reasons, nonmigratable data is never migratable (except during data recovery), migratable data should *always* be accessible to the authorized user.

Accessibility also imposes requirements for ready exportability of data. Some users will need assistive technology. While respecting a data owner's rights, the protection sought by a content owner must not be allowed to constrain the modality of the user's interaction with the data. People with disabilities must not be kept from converting content that is available to their peers without disabilities.

By providing a more effective mechanism for data owners to enforce their intellectual property rights, TCG technologies may be used to significantly alter the balance of power in current practices in the usage of information. However, it is important to understand that TCG technologies and mechanisms were designed with a strong bias towards supporting implementations that follow the design principles discussed in this document. As a result, in the particular case of widely distributed commercial content, TCG-enabled deployment can more readily respect established principles regarding use of information and practices of data ownership.[8]

[8] Note that data ownership practices vary by geography.

Controllability Principle

Each owner should have effective choice and control over the use and operation of the TCG-enabled capabilities that belong to them; their participation must be opt-in. Subsequently any user can reliably disable the TCG functionality in a way that does not violate the owner's policy.[9]

The TCG security model enforces the owner's security policy using TCG mechanisms. It is therefore natural that the owner will have the ultimate choice over the use and operation of the TCG-enabled capabilities. It is also the owner whose positive action is required to allow any other party to use any part of the TCG functionality – for instance, to perform a "remote attestation" or to gain control of a part of the protected storage (for instance, to store software licensing information). This principle of owner control is fundamental to the TCG specifications.

Designers of systems using TCG-enabled capabilities should not compromise the effectiveness of such control by the owner, for instance by reducing the owner's effective control to a single all-or-nothing participation. Such a modification that effectively removes owner control is contrary to the TCG principles. The TCG specifications have been developed to permit the owner to delegate arbitrary subsets of owner capabilities to the user. However, the owner still retains overriding control and can revoke delegation at any time.

On the other hand, those building systems using TCG-enabled capabilities should provide the user, as far as it is possible, with appropriately detailed control. For example, adherence to the TCG Privacy principle suggests that where any personal information concerning the user will be included in a remote attestation, the user should have effective means to control such inclusion. This control is *in addition* to the facilities that the TCG specifications provide for the user to disable the operation of the TPM entirely until the overall system is restarted.

TCG anticipates that there may be devices with multiple owners including cell phones, other peripheral devices, and servers, and that this split ownership complicates the issue of controllability. This is why TCG has included the fundamental principle that each owner should have control only over those functions that are appropriate for their ownership. It seems likely that the best solution for controllability in the situation of multiple ownership is segmenting TPM functionality. As an example, in some domains there will be mandatory security functions that will always be activated and other TPM functionality controlled by other owners of the device that may or may not be activated, depending on the situation.

It is important that TCG technology not be used to coerce the use of the technology. TCG features could potentially enable a situation in which users are essentially "forced" to use the TCG mechanism in order to have access to a set of services. This could result from "bundling" — where a single large provider of services could use

---

[9]The concern for owner and user controllability is another reason for the deliberate absence of a single TCG root (discussed also in footnote 6).

the combination of its role as a major provider with the TCG remote attestation capability to ensure that the user is employing a configuration that the provider insists upon, even when there is no security reason for such a choice. Another situation that can arise is where a significant portion of the providers of a particular service could use their market clout (the fact that they constitute a majority of providers of that particular type of service) to essentially *force* the use of TCG technology. As a consequence, users who do not choose to employ TCG technology would be essentially unable to access that service.[10] **The TCG believes that such behaviors are inappropriate uses of the TCG technology**. **The use of coercion to effectively force the use of the TCG-enabled capabilities is not an appropriate use of TCG technology.** However, preventing potentially coercive and anticompetitive behavior is outside the scope of TCG.

Particular principles that follow from the top-level controllability principle are the following:

- Appropriate notice to the user of the entity requiring the security policy.
  Since a TCG-enabled system is enforcing the policy of the platform owner, it is appropriate that each user has effective notice of the entity making this requirement. Additionally, this entity should provide explanation for those aspects of the owner's policy that may reasonably be expected to affect the user. Such notice may be particularly important where the expected users are members of the public – for instance in a library, public-access terminal, Internet café, or similar environment. The form of the notice will likely depend on specific implementation of the TCG technologies and the environment in which it will be used.

- TCG-enabled capabilities are opt-in.
  The decision for a platform owner to use TCG-enabled capabilities should be one of positive assent. The ability of the user to suspend TPM–enabled operation should not be blocked; the consequences of opting out should be made clear to the user and should not extend beyond the minimum required by the owner’s security policy.

- At any time, at the discretion of the user, a nontechnical user should be able to easily determine the operational state of the TCG-enabled capabilities. Depending on the environment and specific implementation of the TCG capabilities, this may be facilitated through the user interface or an appropriate notice of the state of the TPM-enabled capabilities.

- Fine grained control of transactions as appropriate per application.
  In order to allow the flexibility that some applications will require, the TCG

[10]Clearly there are domains, such as the financial industry, for which the requirement of TCG-enabled technology is completely appropriate to provide the required level of security.

specifications provide for fine-grained control of the use of TCG-enabled capabilities. [11]

The last guideline above – fine-grained control – can frequently be in conflict with the final top-level principle below: ease-of-use. Applications that constantly require the user to authorize each step of every transaction will be deservedly unpopular. It is nevertheless appropriate for the TCG specifications to provide, as they do, for a fine level of control, as it is necessary for certain applications. Of course, it is only at the application or service level that it is possible to determine, in the context of the user's and owner's goals, which TCG-enabled transactions can be considered “trivial” and which ones “significant.” It is important that there be appropriate notice for the significant transactions.

Ease-of-Use Principle

The nontechnical user should find the TCG-enabled capabilities comprehensible and usable.

Balancing security and ease-of-use is, in itself, a largely unsolved problem in practice: the prevalence of passwords written on Post-It® notes on users’ screens is one of many illustrations. Given the wide disparity of users’ capabilities and behavior, when TCG adds in the TCG privacy and controllability principles, the challenge of addressing all these concerns while preserving ease-of-use becomes quite considerable. Nevertheless, application designers will need to strive to achieve such a balance. One possible mechanism is the creation of profiles for security, privacy, and controllability with settings that meet anticipated typical user needs but that can be refined or customized as desired.

Given the challenge of balancing security and ease-of-use, TCG strongly recommends that human interface experts be involved early on in the process of designing TCG-enabled systems, even those that do not directly interface with the user, since even those may end up with requirements on the user. Effective user control requires ease-of-use; therefore, these concerns must be considered from the beginning of the design process.

In the case where user control must be fine-grained or where ease-of-use design has been less than successful, TCG-enabled technology may be quite difficult for users with limited technical capabilities to employ. While in large organizations, such users will have an IT department to take care of implementation, private citizens and small businesses will not. Thus, there is likely to develop a thriving consulting business in the implementation of TCG security features. This model is quite

[11] For example, each cryptographic key in the storage hierarchy has a separate authorization value, which must be matched in order to access further keys and data protected by that key. Creators of systems that build on TCG-enabled capabilities should not arbitrarily coarsen this access control (for instance, by storing logically separable categories of data under a single key). Rather, they should provide convenient, secure methods to allow owners and users to specify control at various levels of detail, as appropriate to the particular application.

reasonable so long as users have a genuine choice of consulting services. Care should be taken by those enterprises that require users to have TCG-enabled technologies in order to obtain service. Developers and implementers of TCG-enabled technology should make careful design decisions and not unnecessarily limit the breadth of user choice.

Conclusions

Computing and the Internet have fundamentally changed the value and importance of information. TCG technology, when properly implemented, has the capability to greatly improve the security of platforms on the Internet. At the same time, as with most security technologies, TCG technology could also be used inappropriately to undermine basic human rights of privacy and platform owner/user control. In light of this possibility for misuse of TCG technology, the TCG has worked very hard to specify building blocks for a security system that favors platform owner/user control, user privacy, interoperability, and data portability. The TCG realizes that market forces, coercive behavior, and poor implementations can do much to weaken these principles and that there is little the TCG organization can do to prevent a manufacturer or system designer from subverting the goals of privacy and control, if they are determined to do so. What TCG can do, however, is to say that such implementations fit neither the spirit of the TCG organization nor the letter of the TCG Principles.

The fundamental goals of the TCG organization are: security, user privacy, interoperability, and controllability. Portability of data and ease-of-use are techniques that are critical in the furtherance of these goals. The specific principles in this document are meant to provide clear direction on what is needed for a TCG-enabled implementation that respects these fundamental goals.

The companies' members represented in the TCG have developed these principles as a reflection of their objectives and values in developing the TCG specifications. The TCG states these principles and best practices to guide those implementing the specifications.