Mobile Phone Work Group

Use Case Scenarios – v 2.7

Abstract

This document describes use cases for the application of Trusted Computing Group (TCG) techniques and specifications to mobile devices. It has been written to guide subsequent technical specification work within the Mobile Phone Working Group (MPWG) of the TCG. It has also been written to provide parties outside the TCG with a description of the work being carried out by the MPWG.

Terms and conditions for use of TCG documents can be downloaded from https://www.trustedcomputinggroup.org/about/legal/

Contents

1 ABOUT THIS DOCUMENT 2
1.1 Introduction 2
1.2 References 4
1.3 Terms and Abbreviations 5
1.4 Actors 6
2 USE CASE SCENARIOS 7
2.1 Platform Integrity 7
2.2 Device Authentication 9
2.3 Robust DRM Implementation 11
2.4 SIMLock / Device Personalisation 14
2.5 Secure Software Download 16
2.6 Secure Channel between Device and UICC 18
2.7 Mobile Ticketing 20
2.8 Mobile Payment 23
2.9 Software Use 26
2.10 Prove Platform and/or Application Integrity to End User 28
2.11 User Data Protection and Privacy 30

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

1 ABOUT THIS DOCUMENT

1.1 Introduction

Existing Trusted Computing Group (TCG) specifications were not written with mobile devices in mind. However, the Mobile Products Working Group (MPWG) believes that by adapting these specifications and generating profiles that place the specifications' building blocks in a "real-world" context, readers will see how the specification can work with mobile devices. These Use Cases intend to outline possible uses of the future TCG specifications that may be deployed to serve the use of mobile devices. The use cases described may or may/not be implemented or supported by the specifications at the time of specification release.

These use cases lay a foundation for the ways:

- MPWG will derive requirements that address situation described in the use cases.
- MPWG will specify an architecture based on the TCG architecture that will meet these requirements
- MPWG will specify the functions and interfaces that will meet the requirements in the specified architecture.

All use case summaries focus on solutions rather than implementation details. Because these case scenarios all share the same building blocks of TCG's trusted architecture in their solution, readers will see how these same components overlap to serve different functions. For example, requirements and technical details relating to the "DRM Implementation" Use Case will invoke similar details as found in "Platform Integrity" and "Device Authentication" Use Cases.

The use case format is adapted from work by Alistair Cockburn [1]. Each Use Case contains the following elements:

- Characteristic information
    - Goal in context (what the use cases aims to achieve)
    - User Benefits
    - Relevant to (types of mobile devices impacted)
    - Preconditions
    - Success End Condition
    - Failed End Condition
    - Primary Actors
    - Trigger (what event or conditions initiates the opportunity)
- Lifecycle
- Variations
- Threats
    - If and how these threats are met by the use of trusted computing

One aspect of lifecycle is common to all Use Cases: the end of life of the Device itself. For privacy reasons, any identities belonging to the Device as a whole, and any associated security data (keys etc.) should be deleted so the data cannot be recovered. In addition, any security data that is linked to the User or to the User's consumption of various services must be deleted from the Device, although such data might first need to be migrated onto the User's subsequent Device. The old Device can then be recycled

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

in a completely fresh state, or it can be physically destroyed, parts recycled etc. Some of the individual Use Cases have their own special end of lifecycle considerations.

1.1.1 Types of use case

There are two types of Use Cases in this document: "Substantive" and "Application Specific".

Substantive Use Cases describe functionality *that is likely to be required of all devices* implemented according to MPWG's technical specifications, due in late 2005 release. For these use cases MPWG will cite not just enablers for the use case, but also present how problems unique to the use case are solved. There is one substantive use case in this document: Platform Integrity, page 9.

Application Specific Use Cases describe functionality *that may not be required of all devices* implemented according to the technical specifications that MPWG will produce. For these cases, MPWG may specify generic functionality (for example, secure key storage and use) that can be used to enable a specific use case, but not specify the actual functionality of the use case itself. However, some of these use cases, if considered sufficiently important, may be as fully specified as the substantive use case. The application specific use cases in this document are those use cases that are not substantive (as of 5-05, only "Platform Integrity" meets this criteria).

1.1.2 Why are standards needed?

One might argue that standards for trusted computing, whether for mobile phones or other platforms, are not needed. And that given the reasonably small number of relevant hardware and software providers, vendors should just agree on details amongst themselves. However, members of the TCG/MPWG believe that trusted computing standards for mobile phones are required and beneficial for the following reasons:

1. **An Industry-vetted solution** – An open standard undergoes extensive scrutiny during its formative stage. Such close examination, dialogue and input by industry experts and vendors who will support the new standard ensure that the final specification best meets its intended objectives, with a minimum number of security flaws.
2. **Built-in Industry-wide Compatibility** – The wide use of a standard lowers risks to hardware vendor and terminal suppliers that choose to support the standard's required functionality. Companies adopting the standard can be confident that their products will readily integrate with other entities in the TCG value chain and can assimilate quickly into a ready market.
3. **Freedom to Choose Among Sources, Less Risk** – Presently, terminal suppliers cannot easily change hardware providers because software often is optimized for one chipset and supports only that chips' functionality. The MPWG specification ensures consistency in the security software/hardware interface, which not only simplifies product design and assures interoperability, it also stimulates competition and creates purchasing options.
4. **Problems Identified by Informed Consensus** – The MPWG standard unites the industry to collaboratively decide and address priorities, as well as develop a common understanding of the most important TCG concepts. In contrast, without standardization, there is a greater risk of insular and fragmented decision making that may undermine larger security objectives and efforts.
5. **All Know More Together, Than One Knows Alone** – Trusted computing is narrow field with few experts. Creating a standard based on the input of all relevant market segments will attract recognized trusted computing industry experts. And as a group possesses more knowledge than any one company, hardware vendors will learn what problems need to be solved first and then build appropriate standard-compliant solutions, rather than creating a proprietary design that may not perform as well across as wide a range as a standard.
6. **Easier, Faster Product Design and Rollout** – The use of standards in the design process speeds product developments and lowers costs involved in certification. Manufacturers can execute on their best ideas faster and gain the critical first-to-market advantage.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

1.2 References

This document refers to the following external document.

Reference	Description and Location
[1]	Use cases adapted from Alistair Cockburn at http://alistair.cockburn.us/usecases/usecases.html.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

1.3 Terms and Abbreviations

This document uses the following terms and abbreviations.

Term	Description
AIK	Attestation Identity Key
CA	Certification Authority
CMLA	Content Management License Administrator http://www.cm-la.com/
CRTM	Core Root of Trust for Measuring
CRTV	Core Root of Trust for Verification
DRM	Digital Rights Management
ETSI SPC	European Telecommunications Standards Institute – Smart Card Platform
GSM	Global System Mobile
HW	Hardware
IMEI	International Mobile Equipment Identity
ME	Mobile Equipment
MeT	Mobile Electronic Transactions organization. See http://www.mobiletransaction.org.
Mobile TPM	A TPM adapted for mobile phone
MPWG	Mobile Phone Workgroup
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance http://www.openmobilealliance.org
OS	Operating System
OSGi	Open Services Gateway Initiative http://www.osgi.org
PCB	Printed Circuit Board
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
Repurpose	Modifying a Device to perform differently than intended (e.g. Linux on Game Console).
RIM	Reference Integrity Metric
ROM	Read Only Memory
RTM	Root of Trust for Measuring
RTR	Root of Trust for Reporting
RTS	Root of Trust for Storage
RTV	Root of Trust for Verification
RTVI	Root of Trust for Verification Identifier
RVA	Root Verification Authority
RVAI	Root Verification Authority Identifier public key configured in the CRTV for the platform root security authority.
SIM	Subscriber Identification Module

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

SoC	System on Chip: primary platform host execution engine
SW	Software
TCG	Trusted Computing Group http://www.trustedcomputinggroup.org
TIM	Target Integrity Metric
TPM	Trusted Platform Module
TSS	TCG Software Stack
TTP	Trusted Third Party
UICC	UMTS Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
USIM	Universal SIM
3GPP	3rd Generation Partnership Project http://www.3gpp.org

1.4 Actors

In the document the following terms are used to describe certain actors in the use cases.

Actor	Description
Content Provider	The legal owner of content that requires protection using DRM.
Corporation	An enterprise that may support mobile devices as a means to access corporate data and networks.
Device	An entity comprising a platform with one or more Mobile TPMs for which attestation data may be provided
Device Owner	The legal owner of the Device. The Device Owner is entitled to customize the platform. The owner may be a consumer, an IT Administrator for a Corporation or some other entity.
Device Manufacturer	The manufacturer or brand of a Device – typically an OEM
End User	The user of a Device. The End User may or may not be the Device Owner.
Employee	An employee using a mobile phone to access applications, data and networks of the Corporation employing him or her.
Service Provider	An entity that wishes to discover properties of a trusted mobile phone platform and provide services to that Device.
Network Provider	An entity that provides cellular communications functionality to the platform (e.g., a 3GPP network provider.)
Application Provider	An entity generating and/or selling user applications to be executed on the platform
Attacker	A person or organization trying to circumvent some policy of the Device, the Service Provider, the Application Provider or the Network Provider

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2 USE CASE SCENARIOS

2.1 Platform Integrity

2.1.1 Characteristic Information

Goal in Context: To ensure devices possess and run only authorized operating system(s) and hardware. For example, an unauthorized operating system can be a modified version of the original operating system. Such modifications might broadcast false device identification data (e.g., a false IMEI code), by either altering broadcast program code, or by changing memory contents or location(s). Unauthorized hardware could be an extra component that is inserted to change or block signals on the device's data buses.

Maintenance of platform integrity means that platform hardware and principal elements of the platform software (e.g., boot code, OS kernel) are in the state originally set by the device manufacturer.

User benefits: The end user (eg End User or Corporation) may be able to rely upon the trustworthiness of their Device and that their Device will be able to defend itself against malware (e.g. viruses, worms, spoofs). Platform Integrity also benefits the User in that it is a key building block for all the other Use Cases in this document. For example, privacy of User data is impossible without data protection, which depends on platform integrity; thus, stronger platform integrity enables stronger data privacy.

Corporations and their Employees will benefit because the mobile phone can be supported as platform for corporate applications. It can be allowed on the corporate network and it can be allowed to handle and store corporate documents. This will usually not be acceptable for a Corporation unless it can assume that confidential information and the corporate network will be safe.

Relevant to: Phones, PDAs, and any embedded device that can be repurposed.

Preconditions: Device is powered off or in some other predetermined initial state (for the boot time platform integrity check so that the boot time platform integrity check is performed when the device is booted). The device has not been tampered with.

Success End Condition: Device boots up normally with assurance that platform integrity has been maintained. Additionally, platform integrity checks may take place when the device is operational, again providing assurance that platform integrity has been maintained. These "run-time" integrity checks might have been performed before security-relevant operations are performed, such as before device software upgrades.

Failed End Condition: The attacker modifies platform software. Platform integrity checks fail and the device boots normally.

Primary Actors: End-user, device, device owner, device manufacturer.

Trigger: Device power up or creation of initial state within device, or request for significant run-time operation requiring platform integrity check.

2.1.2 Lifecycle

Lifecycle stage	Activities undertaken during this stage
Device manufacture and/or initialization	Data, policies and keys essential for platform integrity are securely provisioned onto the device when the device is in an approved state and possibly in a controlled environment.
Boot time	Platform integrity is checked, either in its entirety or the integrity of selected portions of the platform.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

Prior to significant run-time activities	Platform integrity is checked, either in its entirety or the integrity of selected portions of the platform.
Authorized platform upgrade	Platform software and/or hardware are upgraded in an authorized and controlled manner. Data, policies and keys that are essential for platform integrity are also upgraded in an authorized and controlled manner.

2.1.3 Variations

Instead of checking the whole device OS for performance enhancement, only some of the main OS is first verified. Then, at run-time, other security-relevant parts of the OS are checked before being executed.

2.1.4 Threats

1. The logic of the device firmware is modified.
2. The device hardware is modified.
3. The device functions in a manner other than intended by the device manufacturer.
4. The device is modified such that it broadcasts false device identification (e.g., a false IMEI code).

2.1.4.1 How does the use of TCG specifications mitigate threats?

As stated in the Introduction, safeguarding platform integrity is a pre-requisite for all subsequent use cases in this document. It is therefore the intention of the MPWG that mechanisms and enablers for platform integrity will be specified.

Threats (1) to (4) may result from lack of data or insufficient data within a device to record what the desired condition of the platform should be, and lack of mechanisms capable of checking that this desired condition is maintained. Use of TCG specifications specifying these data are present and mechanisms are in place will ensure complete and robust device implementations sufficient to maintain integrity and/or detect unauthorized modifications and take specified actions as a result.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.2 Device Authentication

2.2.1 Characteristic Information

Goal in Context: There are two sub-goals to this use case.

First, device authentication may be used to assist in end-user authentication in that the device can store and protect identification information, such as keys, that can be used to securely authenticate the identity of the device to a service provider or a network provider and where that device identity has been bound to an end user in some unspecified way.

Secondly, device authentication may prove the identity of the device itself, and not assist in end-user authentication in any way.

Both kinds of authentication might be required in DRM.

In the context of authentication to a service provider or a network provider, there may be multiple identities. Some of these identities can be both end-user and device identities. The device should be able to store and protect all such end-user and device identities and use the appropriate identities depending on the context.

User Benefits: In some cases, the User will be better served by the Service Provider who trusts in the User's Device, and the amount of services the User can benefit from should therefore increase. Device Authentication does not necessarily reduce the User's privacy since the User can still be in control of which Service Providers their Device authenticates to and can make this decision based upon knowledge of the Service Provider's privacy policy for example. Further, Device Authentication can be designed to reveal no information about the User's Personal Id, so enhancing privacy in some cases.

Robust Device Authentication can also be used as part of an overall strategy against Device theft. This benefits the User by making the Device less attractive to steal.

Relevant to: Phones, PDAs, and any embedded device.

Preconditions: The device has intact and unique identification information. An authentication request is received by the device.

Success End Condition: Identities cannot be cloned or modified. An identity stored in the device is used to authenticate to the service provider. The service provider grants or denies the service and/or content being requested. No two devices/end users can have the same identity.

Failed End Condition: An attacker extracts keys or data from the device so that another device can masquerade as the original device.

Primary Actors: End user, device, service provider or other device requesting authentication

Trigger: Authentication request from the network provider or the service provider.

2.2.2 Lifecycle

Lifecycle stage	Activities undertaken during this stage
Device manufacture and/or initialization	Data, policies and keys related to device identity are securely provisioned onto the device.
Boot time and prior to significant device authentication events.	Platform integrity is checked, to ensure that the data, policies and keys related to device authentication have not been modified in an unauthorized manner.
Device authentication events.	Device performs authentication protocols so as to prove its identity to service providers or network providers and thereby gain services or privileges requested from these providers.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.2.3 Variations

There can be multiple identities in the same device.

2.2.4 Threats

1. The identity is spoofed in order to get unauthorized access to services.
2. Identity is no longer uniquely bound to the device.
3. Theft of mobile equipment.
4. Device authentication is used to track the device. This is a potential privacy threat.

2.2.4.1 How does the use of TCG specifications mitigate threats?

Threats (1) to (3) result from insufficient protection of the data, policies and keys on the device that are used to authenticate the device. TCG specifications will specify methods to securely and robustly store and use data, as well as policies and keys that are used to authenticate the device so that these cannot be obtained by attackers (or at least can only be obtained with great difficulty so that the time and effort expended by the attacker provides sufficient time for the end user/network provider/service provider to reduce or negate the impact of the attack).

Threat (4) is mitigated by applying TCG technology specifically designed to protect against privacy threats.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.3 Robust DRM Implementation

2.3.1 Characteristic Information

Goal in Context: Both service and content providers need assurance that device implementations of DRM specifications (e.g., OMA DRM Version 2) are robust and can be trusted to protect their digital content. (Robust here means resistant to an acceptable level of attack.) TCG specifications do not define a DRM system, but do provide enablers which can be used within DRM systems.

Currently, for some DRM specifications there exists a "trust model" that specifies in generic terms how robust DRM implementations should be. However, by employing trusted computing principles, techniques and specifications, device manufacturers can gain additional direction on steps necessary to establish and quantify the security of a robust implementation of the DRM specification. Manufacturers can then declare and self-certify that they have correctly met the requirements. Such conformance will also assure service and content providers that their interests are protected, and also make it easier for them to assess whether client devices are robust or not. This assurance may mean that the DRM implementation qualifies for receiving DRM-protected content (e.g., CMLA license).

User Benefits: The User can benefit from robust DRM implementation because it can enable valuable content to be distributed to mobile Devices with the permission of the Content Providers. This is because assurances can be given to Content Providers that their content will be protected on such Devices. For a variety of reasons, mobile Users may be more willing to use distribution channels that act with the Content Providers' permission than ones which do not, and to that extent will benefit from the existence of approved channels, provided they are made sufficiently attractive.

Also, DRM technology can protect the User's own content. For example it can encourage Users to share pictures, messages etc., without risking that they will be distributed all over the Internet.

In a corporate environment, an Employee will benefit by being allowed to access sensitive company information on the Device everywhere and anytime. Document control technology (enabled through Trusted Computing) can make sure that documents are treated according to the Corporation's policies (for example cannot be copied or sent). A Corporation will benefit by being able to mobilize its Employees without additional risk to its data and networks.

One fear is that a DRM implementation reduces the Device's capabilities. However, good DRM specifications typically do not control content that is not DRM protected; robust DRM implementation does not therefore mean that the User's use of unprotected content will be affected in any way. Nevertheless, TCG can only provide enablers for DRM solutions; it cannot force implementation of good solutions.

Relevant to: PDAs, mobile phones, and other mobile devices implementing DRM.

Preconditions: None specified.

Success End Condition: A hardened implementation of the DRM specification set may be achieved and that all parties involved can be assured of this hardened implementation.

Failed End Condition: An attacker accesses a particular item of DRM-protected content in violation of the policy assigned to the device and the DRM-protected content.

Primary Actors: User; device; device manufacturer; service provider; content provider.

Trigger: Here is a non-exhaustive list of potential triggers:

- The platform user requests registration with a service provider;
- The platform user makes a request for a rights object/license associated with protected content from a service provider;
- An integrity check of device software related to DRM is attempted;

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.3.2 Lifecycle

Lifecycle stage	Activities undertaken during this stage
Device manufacture and/or initialization	Device-specific keys are securely generated within or provisioned onto the device when the device is in an approved state and possibly in a controlled environment. System information (e.g., policy files, root public key certificates) are securely provisioned onto the device when the device is in an approved state and possibly in a controlled environment. Software relating to DRM is securely loaded into memory when the device is in an approved state and possibly in a controlled environment.
Boot time	Integrity of software and data, including keys, is checked.
Run time	Device-specific keys are securely used, as intended, during DRM operations. DRM-specific data (e.g., rights objects, content keys) is securely obtained and stored within the device.
Device renewal (if appropriate)	DRM software or data is securely updated (by authorized entities only).
Termination of DRM service	The Device's association with a Rights Issuer terminates, or it leaves the "trust model" entirely. DRM specific credentials will need to be deleted from the Device or invalidated. Whether this affects content stored on the Device may depend on the rights purchased within the DRM system e.g. whether they were based on subscription or permanent usage.

2.3.3 Variations

None listed here.

2.3.4 Threats

A number of threats result from and impact devices that are not robustly implemented:

1. Keys related to DRM (content encryption keys, for example) can be extracted from the device and used to decrypt protected content in an unauthorized manner.
2. The key used to authenticate the device to service providers can be extracted and used to clone the device.
3. The data contained with rights objects/licenses stored on the device can be manipulated in an unauthorized manner.
4. The software relating to DRM on the device (including elements of the main OS used by DRM applications) can be manipulated in an unauthorized manner or additional unauthorized software can be added so as to allow unauthorized access to protected content.

Threats to the business are possible if assurance of robustness of implementation cannot be given to service and content providers and if clear guidelines are not given to device manufacturers:

5. A service provider or content provider is bewildered by the many possible implementations of a standard DRM specification for which there are no guidelines regarding implementation and, therefore uses only a subset of the possible implementations on the market.
6. Device manufacturers have to spend time evaluating how robust their implementations must be and developing their own techniques for robust implementation as there are no clear guidelines and techniques for robust implementation.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

7. A small number of non-robust implementations of a particular DRM standard appear and give a bad reputation to that standard.

2.3.4.1 How does the use of TCG specifications mitigate threats?

Threats (1) thru (4) of this use case are technical threats resulting from poor implementation of a DRM specification. The use of TCG specifications mitigate these threats in that TCG specifications will define how a robust implementation of DRM can be built using established TCG commands and architectures. In particular, the use of TCG specifications should ensure that the implementation is resistant to software attacks, for which DRM implementations are often not resistant.

Threat (5) is also a technical threat resulting from poor implementation of a DRM specification but with commercial impact. It is mitigated as for threats (1) to (4).

Threats (6) and (7) are “commercial” threats resulting from lack of assurance to content and service providers of device robustness and lack of guidance to device manufacturers on device robustness requirements, respectively. The use of TCG specifications mitigates threat (5) in that device manufacturers can certify that their implementation is built according to TCG specifications thus providing assurance of robust implementation to those service and content providers that trust TCG specification and certification. Threat (6) is mitigated as the device manufacturer can consult TCG specifications in order to seek guidance on robustness requirements.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.4 SIMLock / Device Personalisation

2.4.1 Characteristic Information

Goal in Context: The primary goal is to ensure that a mobile device remains locked to a particular network (or network subset, service provider, corporation or (U)SIM) until it is unlocked in an authorized manner.

This goal originates from two fundamental scenarios:

- Network providers and indeed device users need to be assured that mechanisms to deter Device theft are in place such that stolen Devices become less valuable for re-use and re-sale.
- Entities, for example network providers or service providers, who subsidize the cost of devices, need to be assured that end users cannot move their device to another network provider or service provider before the agreed subscription contract has been upheld, without authorization from the subsidizing entity.

User Benefits: Secure SIMLock benefits the User in a number of ways. Primarily, it enables the User to obtain a Device at a substantial discount to the true supply cost. This expands the User's purchase options rather than reducing them. Users still have the option of buying a full-price, unlocked phone, and network operators must allow a locked phone to be unlocked later, after the cost difference has been recovered.

Another benefit is that a User can voluntarily lock a Device to their own SIM – this enables the User to then personalize the Device (with content, private data etc.) while preventing anyone else using it.

A third benefit is that SIMLock can be used as a part of an overall strategy against Device theft, making the Device less attractive to steal.

Relevant to: Mobile phones and other subscription related mobile equipment.

Preconditions: End user has in his possession a mobile device which is locked to a particular network, network subset, service provider, corporation and/or (U)SIM.

Success End Condition: The device remains locked to a particular network, network subset, service provider, corporation or (U)SIM.

As a consequence of this:

- If handset theft occurs, the ME will be less re-useable or re-sellable (when SIM Locking is used in conjunction with other security mechanisms such as IMEI protection and EIR implementation) than if the ME personalization was not operational.
- The user of the mobile equipment cannot move their phone to another network or service provider for example, before the agreed subscription contract has been upheld, without authorization from the current subsiding entity, be it the network provider or current service provider.

Failed End Condition: Unauthorized unlocking of the device, where the device can be used on an alternate network or service.

Primary Actors: End User; Device; Device Manufacturer; Network Provider

Trigger: Sale of subsidized mobile equipment.

2.4.2 Lifecycle

Lifecycle stage	Activities undertaken during this stage
Device manufacture and/or initialization	Data, policies and keys are securely provisioned onto the device (and to the USIM).

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

	Software relating to SIMLock is securely loaded into device memory.
Boot time, prior to authorized unlocking of SIMLock	Integrity of SIMLock software and data, policies and keys, is checked. SIMLock software checks that USIM inserted into device is allowed by provisioned policies, and allows or forbids access to network provider services accordingly.
Unauthorized attempt to unlock SIMLock	Device resists unauthorized attempt to unlock SIMLock by, for example, rejecting unauthorized request to change software or policies, or to access SIMLock keys.
Authorized unlocking of SIMLock ("depersonalization")	Unlock message is received from authorized entity (which demonstrates authorization, for example, by inserting correct keys or passcodes) and SIMLock policies are changed.

2.4.3 Variations

None.

2.4.4 Threats

1. Device software or data is changed in an unauthorized manner such that SIM Lock is no longer in (correct) operation.
2. Secret unlock codes stored on the device or computed from data on the device or stored on the SIM/USIM are revealed to unauthorized entities so that the device can be unlocked in an unauthorized manner.
3. Secret unlock codes are revealed to unauthorized parties by insider attackers within a device manufacturer or network provider.

2.4.4.1 How does the use of TCG specifications mitigate threats?

Threats (1) and (2) result from a poor implementation of SIMLock whereby unauthorized entities are allowed to change/access device software or data that they should have no access to. The use of TCG specifications should help ensure that poor implementations are not produced and therefore that correct access control to SIMLock software and/or data is observed.

Threat (3) cannot be met by TCG specifications under current methods of SIMLock and Device personalization, which require the use of secrets stored by a device manufacturer or network provider.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.5 Secure Software Download

2.5.1 Characteristic Information

Goal in Context: The user wants to securely download application software or updates, firmware updates or patches. "Application software" refers to significant applications that are probably installed into the device's native OS, such as DRM agents or browsers, and not to applications, such as games, which may run in a specific execution environment within the device.

It may also be the case that the device manufacturer or network provider wants to install firmware updates or patches on the device, for example, in case of a security flaw in the firmware.

The application software/upgrade/patch download is conducted with the appropriate security and the application software/upgrade/patch operates correctly and with the required authorization and privileges once it has been installed.

User Benefits: The User benefits in the same way as with signed software on PCs. The process of signing reduces the chance of malware such as viruses, worms etc., as the originator of the software may be traced and action taken against them if it contains malware. The software is also protected from change by anyone else who might try to insert malware.

Specific benefits of Trusted Computing are reduced User inconvenience and risks, and increased User assurance. The Device can be safely set up to automatically trust certain software and so reduce the number of decisions the User has to make. Names and organizations the user knows can be reliably shown as the software originator. And through increased Platform Integrity, Trusted Computing can reduce the risk that the whole secure download process is tricked or bypassed.

For many corporate uses it is a prerequisite that the Corporation's IT organization is able to securely manage software on the Device. Trusted Computing will support these uses through enabling a more secure software download.

Relevant to: Mobile phones and possibly PDAs.

Preconditions: User, device manufacturer, or network provider tries to download application software, firmware updates or patches.

Success End Condition: The device securely downloaded application software or a software update.

Failed End Condition: An attacker modifies the application software in transit to the Device.

Primary Actors: Device user, device manufacturer, network provider, software provider

Trigger:

- The user tries to download application software or a software update.
- The device manufacturer wants to install a security patch on the device.
- The network provider wants to install a security patch on the device.

2.5.2 Lifecycle

Lifecycle stage	Activities undertaken during this stage
Device manufacture and/or initialization	Data, policies, keys and program code relating to software download are securely provisioned onto the Device when the Device is in an approved state and possibly in a controlled environment.
Boot time and at run prior to significant software download event.	Integrity of data, policies, keys and program code relating to software download is checked.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

Software download event	Software is downloaded according to the policies and program code on the device.
Device renewal (if appropriate)	Software update policy can be securely updated (by authorized entities only).
Termination of download service	The Device must be no longer updateable by a previously authorized entity (e.g. because of change of network provider or corporation). Keys and privileges that the Device associates with that entity are destroyed.

2.5.3 Variations

None

2.5.4 Threats:

1. The application software or the software update is malicious, and may contain worms, viruses, etc and yet is given access to significant device functionality.
2. The software update is faulty and introduces loopholes in the device operating system that can be exploited by worms and viruses.
3. The application software or the software update is modified in an unauthorized manner.
4. The firmware update (for instance, a patch) is analyzed by an attacker in order to reverse engineer the software and so determine the operation of the firmware (for example, to find security flaws in the software).
5. The update violates the download policy of the device (e.g., user installs an older version of the firmware or an older version of a DRM agent).

2.5.4.1 How does the use of TCG specifications mitigate threats?

TCG technology can be used to specify enablers which can be used to verify the integrity of the software (and any authorization it has been given) which is about to be installed. For example, TCG can specify cryptographic services that can be used to verify certificates and to control the authorization that use of the certificate implies. Keys (public CA root keys), which are used in this verification process can be securely provisioned and integrity protected by TCG technology. Threat (1) can be met in this way. Similarly, TCG can specify enablers that can be used to protect the integrity and confidentiality of software updates, thereby meeting threats (3) and (4).

TCG specifications can be used to specify an authorization and privilege architecture for device software so that software updates are given only the functionality they require on the device and no more. Threat (2) can thereby be reduced.

TCG specifications can also be used to specify enablers for the enforcement of download policies, thereby meeting threat (5).

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.6 Secure Channel between Device and UICC

2.6.1 Characteristic Information

Goal in Context: Some security sensitive applications (e.g., an m-commerce application) may be implemented partly in the UICC and partly in the device.

The application is partly in the UICC for various reasons, among which are compatibility with legacy services, to take advantage of the physical security of the UICC and the portability of user credentials that the UICC provides.

In order to avoid malicious software on the device or compromise of the device-UICC interface interfering with the operation of these split applications, the UICC should be aware of the trust status of the device it is inserted in, and it should also be possible for a secure channel to be established between the device and the UICC. It may also be necessary for the device to be aware of the trust status of the UICC.

A second reason for requiring a secure device-UICC channel is for when sensitive data, such as provisioning data, is transmitted from the UICC to the device or vice-versa.

User Benefits:

User friendliness of migration: One User benefit of a secure channel is that it enables the User to store sensitive assets (like a signature key, electronic money or electronic tickets) on the UICC, and then move them between Devices. As the UICC can authenticate each new Device, it can decide whether it is a secure place to use those assets, or else release them to the Device over the secure channel.

This is important when the Device is being changed or fixed, since Users do not want to lose their assets. Alternatively, if the assets are no longer needed, but must be securely deleted, the UICC can be destroyed.

Faster availability of some applications: Another benefit is that Users will generally benefit from fast deployment of security applications if they can be split between the UICC and the Device, with a secure link between the parts. The use of a protected core on the UICC will encourage payment applications etc. as the core will be easier to evaluate: it is on a trusted component already, and relatively stable. The same core functionality, like a signing engine, may be used in several Device applications.

Relevant to: Mobile phones and possibly PDAs.

Preconditions: User wants to use his mobile phone for security sensitive m-commerce applications. These applications are implemented using both the UICC and the device.

Success End Condition: Messages between the device and the UICC are secured and the UICC is given assurance that the device is “trusted”, according to policies on the UICC (for example, the device has been authorized for a particular purpose by some entity related to the UICC and the device is in the condition required as part of that authorization, that is, device integrity has been maintained as required).

Failed End Condition: The attacker inserts a UICC into a device that is not authorized for a particular purpose or into an authorized device that has been modified in an unauthorized manner. Sensitive applications and/or data on the UICC are made available to the device.

Primary Actors: Device, user, device manufacturer, network provider, service provider issuing the sensitive applications or conducting the transaction.

Trigger:

- UICC insertion in the device
- Power up or reboot of the device
- Selection by the user of a sensitive application.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.6.2 Lifecycle

Lifecycle stage	Activities undertaken during this stage
Device manufacture and/or initialization	Data, policies, keys and program code essential for establishment of secure device to UICC channels are securely provisioned onto the device (and UICC).
Boot time and at run time prior to establishment of secure Device to UICC channel.	Integrity of data, policies, keys and program code relating to establishment of secure device to UICC channels is checked.
Event requiring establishment of secure device to UICC channel.	Secure channel is established using the data, policies, keys and program code provisioned on the device for this purpose.

2.6.3 Variations

None listed here.

2.6.4 Threats

1. Device software is malicious. For example, it contains worms, viruses or other harmful software that makes it potentially dangerous for sensitive applications implemented partly in the UICC. One example of an attack is eavesdropping or "sniffing" of the PIN when sent for verification by the device to the SIM/USIM.
2. The SIM/USIM is used to configure the device, but the SIM/USIM may be false and contain false configuration or a malicious application on the device may change the configuration information as it is transported from the SIM/USIM to the relevant area on the device.
3. Stealing of sensitive information, such as keys, by malicious software on the device or between the device and the UICC, while this information is transported between the SIM/USIM and the device. For example, keys used for ciphering of the air interface, or some protected content stored in the device, which are passed from the SIM/USIM to the device may be stolen.
4. The Device is not compliant to relevant specifications but instead is a device solely created to misuse sensitive information stored on a UICC, for example, the device is a UICC reader connected to a laptop running programs designed to extract sensitive data from a UICC.

2.6.4.1 How does the use of TCG specifications mitigate threats?

The TCG MPWG specifications will specify enablers that can be used to build secure and robust implementations of protocols that are used to establish a secure device to UICC channel. The TCG MPWG will **not** specify these protocols, this will be done by other relevant standards groups, for example ETSI SCP. These protocols, implemented according to the TCG specifications, will allow the development of devices that correctly and robustly implement secure protocols for the establishment of a secure device to ME channel. By this means, threats (1) to (4) can be met.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.7 Mobile Ticketing

2.7.1 Characteristic information

Goal in Context: Mobile ticketing is to use mobile devices to download and present tickets.

A ticket is a proof of access/usage rights to a particular service. In this use case, tickets are considered as an electronic data object, that is, an electronic equivalence of paper (plastic) tickets. Tickets can be purchased or redeemed via many mechanisms, for example, phone call, internet, as well as store front. The ticket may be downloaded via any channel to a mobile device at the time it is purchased or redeemed.

The downloaded tickets should not be duplicated or modified in any way to change their rights as purchased.

A ticket presentation is a procedure to prove the possession and validation of such a data object in a mobile Device. We say a ticket is consumed, if it is presented and accepted. This is equivalent to physically punching a ticket. After a ticket is consumed, the rights represented by the data object should be considered as expired.

User Benefits: Mobile ticketing brings User convenience in purchasing tickets from flexible locations and consuming tickets without printing and carrying paper. The tickets can be purchased any time and anywhere. Users don't have to queue up to buy them, or wait for them to be sent through the post. Users are much less likely to lose tickets, or have them stolen, and won't waste time queuing up to use them.

Trusted computing adds privacy and flexibility benefits to the User compared with alternative mobile ticketing approaches. Alternative solutions may require the Service Provider to have a network connection when the mobile ticket is used (to check the ticket is valid and not already used), or tie the ticket to a User's identity at purchase, which may require Users to authenticate themselves at use. The User has no comeback if the Service Provider database is not accessible, or contains an error. The simplicity of a paper ticket (it quickly proves to both the User and the Service Provider the user's entitlement, but nothing else) is not supported.

Trusted mobile devices could enable true parallels for paper ticketing. For example, Service Providers could read tickets off the Device with stand-alone units, and obtain assurances that the tickets had not been forged or duplicated. Users could have assurances that their tickets won't be rejected when they use them. Mobile tickets could be made as anonymous as paper tickets. Once these conditions are met, mobile ticketing can become widespread.

Relevant to: PDAs, Mobile phones, and other Mobile Devices capable of accommodating ticket applications.

Preconditions: None specified.

Success End Condition: A ticketing application which can trustfully reflect the possession, validation, and revocation of the rights as tickets are downloaded and consumed.

Failed End Condition: An implementation of ticketing application is weak and can be attacked so that the rights can be illegally duplicated, modified, or deleted.

Primary Actors: User; Device; Device Manufacturer; Service Provider (acting as a provider of tickets), redeem point, ticket reader/puncher.

Trigger: Here is a non-exhaustive list of potential triggers:

- The platform user purchases tickets;
- The platform user downloads the tickets to mobile devices;
- A ticket is presented and consumed via a local interface such as Bluetooth, RF contactless, etc.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.7.2 Lifecycle

Lifecycle stage	Activities undertaken during this stage
Device manufacture	Device is manufactured with capabilities of verifying the integrity of applications. Ticketing application may or may not be installed as a Device is manufactured. However, the Device has the capacity to provide security services for potential new downloaded applications.
Install ticketing application	Ticketing application is installed to the Device via over the air download, USB port, as well as other media. The platform verifies the authenticity and integrity of the application.
Load tickets to the application	Upon purchasing or redeeming the tickets, the data objects which represent the rights will be securely downloaded to the Device.
Present and consume the tickets	Before the service is accessed, the data objects are presented to a reader for verification before the permissions sought using the ticket is granted. After the permission has been granted, the tickets are considered as consumed.
Termination of ticketing service	The Device is no longer usable with the ticketing application. Security data linked to the application or to its tickets are deleted.

2.7.3 Variations

None listed here.

2.7.4 Threats

After tickets are downloaded to a ticket application, there may not be a record stored in a server for future verifications. The user may not have a long term account with a provider. Furthermore, the tickets may be presented and consumed without real time communications with a centralized database or a server, In other words, the tickets may be verified with an off-line manner. The ticketing application may be modified or some procedures may be bypassed to achieve the following and maybe other purposes.

1. Duplicate tickets in the Device or somewhere else such that the duplicated copies are downloadable and consumable.
2. Recharge (or re-validate) tickets which have already been consumed and the rights represented by the ticket expired.
3. Modify the rights represented by tickets or modify tickets counters.
4. As the tickets can be validated via a contactless interface, an attacker might 'consume' the ticket and the actual user might not know. This attack is equivalent to ticket theft.
5. An attacker interrupts executions of the ticket presenting and consuming protocol in such a way that the actual user cannot use the ticket - this is a form of Denial of Service.

2.7.4.1 How does the use of TCG specifications mitigate threats?

The TCG MPWG specifications will specify enablers that can be used to verify the integrity of the platform so that the ticketing application can be verified for its authenticity and integrity.

The TCG WPWG specifications will assure robust implementations of the ticketing application so that the data objects can not be duplicated, modified, and deleted, thus meeting threats (1) – (3).

The robust implementation of the application also assure the ticketing presenting, verifying, and consuming protocols between the mobile device and the ticket reader can be executed in the way as they

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

are designed so that the interception and interruption of the protocol will not be feasible , thus meeting threats (4) and (5).

MPWG will not specify ticketing presenting, verifying, and consuming protocols but merely provide enablers for robust implementation of the protocols on the Device.

2.7.5 Priority

Medium priority

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.8 Mobile Payment

2.8.1 Characteristic information

Goal in Context: Mobile payment is to use mobile Devices to make payment transaction.

A payment may be made from an account of a credit card, a debt card, or a pre-paid cash portal, a representation of which is stored on the Device. The payment protocol is executed between an application stored in a Device and a point of sale (POS).

A payment with a precise amount must be authorized by the owner of the account. The authorization may be given implicitly or explicitly by the owner. In case of explicit authorization, the owner of the account may, for example, enter a PIN to authorise use of a Device private key to generate a digital signature as a part of the payment protocol.

A payment is a procedure to prove the validation of the account and conduct the transaction. Certain data objects will be transmitted via the Device.

The payment application may be pre-stored to a mobile Device or downloaded to the Device once it is in use in the field. Loading the account information to a mobile device is called personalization. The personalization may be conducted over a wireless interface.

User Benefits: Mobile payment allows Users to use a mobile device as the equivalent of a purse or wallet. The wallet may include Users' sensitive data and data devoted to securing sensitive financial transactions. As for ticketing, this has advantages for the User in terms of convenience. The User doesn't have to carry change, multiple cards etc.

Trusted Computing gives additional User benefits in mobile payment:

1. Fraud risks are reduced, to both User and Service Provider, as payment data and secrets are well protected. Reduced fraud for the Service Provider helps the User too, through greater diversity of Service Providers supporting mobile payment, and lower prices.
2. Privacy is enhanced. The Device may prevent interception and eavesdropping on the payment process, and can provide more anonymity than existing methods of electronic payment (by enabling true equivalents of cash).
3. A general concern with merging the wallet and phone is that it makes the phone more vulnerable to theft. However, where protections against phone theft are enabled by Trusted Computing (see above) these could also protect the User's wallet.

Relevant to: PDAs, Mobile phones, and other Mobile Devices capable of accommodating ticket applications.

Preconditions: None specified.

Success End Condition: An implementation of payment application to precisely reflect the authorization and transaction.

Failed End Condition: An implementation of payment application is attacked and unauthorized transactions occur.

Primary Actors: User; Device; Device Manufacturer; Service Provider; Issuing Bank, merchandise, Point of Sales.

Trigger: Here is a non-exhaustive list of potential triggers:

- The platform user opens a credit card account (or a debt card account, a pre-paid cash account);
- The platform user registers for mobile payment;
- The platform user uses mobile device to pay a merchandise, etc.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.8.2 Lifecycle

Lifecycle stage	Activities undertaken during this stage
Device manufacture and/or initialization	The Device is manufactured with the ability to verify the integrity and authorisation of applications. The Payment application may or may not be installed at the manufacture time. However, the Device has the capacity to provide security services for potential new downloadable applications. If the payment application resides on a smart card, then the Device is manufactured with support for a secure interface with the smart card.
Application provisioning	Payment application is installed to the Device or to a smartcard via over the air download, USB port, or other channels. The platform or the smart card verifies the authenticity and integrity of the application.
Application personalization	Load account information to the payment application by a server via air interface. When a smartcard is used to hold the application, information is delivered to the smartcard via the Device. The account information may be issuer specific. That is, the personalization procedure may happen every time the owner opens a new account with an issuer. The personalization procedure includes a mutual authentication between the application holder and the server. The confidentiality and integrity of the personalization procedure is ensured.
Payment and authorization	A payment transaction is a protocol between a payment application and a point of sale (POS). The protocol includes an authentication of the account and the server and may include an authorization of the payment by the owner.
Termination of payment service	The payment application is removed from the Device, or else the Device becomes no longer usable with a given payment account. Security data linked to the application or that account are deleted.

2.8.3 Variations

None listed here.

2.8.4 Threats

The payment application is attacked to allow unauthorized transaction.

1. The payment application is modified so as to act as a “back door” for non-payment related attacks on the Device.
2. Over-the-air personalization can be intercepted to duplicate an account in other devices or by other media.
3. The confidential information about an account is leaked. As a result, unauthorized payments can be made via other devices or media.
4. If a user needs to input identity or biometrics to activate a payment transaction, then the identity or biometrics data may be intercepted or leaked via the device.
5. For mobile payments that depends on digital signatures for non-repudiation, the private key may be stolen to forge an account owner’s signature.
6. A payment application or a payment account is installed onto an unauthorized Device.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.8.4.1 How does the use of TCG specifications mitigate threats?

TCG technology can be used to measure the authenticity and integrity of the payment application which counters threat (1).

TCG technology can enforce platform integrity so that it can prevent software attacks on the relevant functionality blocks. As a result, the protocols and functions are forced to be executed in the way that was intended. This can be used to counter threats (2)-(4) and (6).

TCG MPWG will not specify the actual protocols and functions but it will specify enablers to allow the robust implementation of these protocols.

A signing key can be created and securely stored using Mobile TPM's protected storage capabilities. This can mitigate threat (5).

2.8.5 Priority

Medium priority.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.9 Software Use

2.9.1 Characteristic Information

Goal in Context: The user wants to securely use an application. I.e., the platform enforces predefined software use policies.

Various different policies should be supported. This means the platform must be able to enforce them. Examples of SW use policies are

a) Each application contains a list of data objects which it is allowed to access. When the SW is executed the platform OS enforces this list. This way a entity different from the application provider can restrict the actions of the SW to a given set of objects. This helps to prevent malicious code from doing bad things.
b) Each application contains a list of functions which it is allowed to execute. When the SW is executed the platform OS enforces this list. This way a entity different from the application provider can restrict the actions the SW is allowed to do. E.g. a game is not allowed to dial any numbers. This prevents a virus or Trojan horse in a game to launch attacks through making calls.
c) After an application is installed to a mobile device, it might need to be revoked due to subsequently discovered software bugs, Trojan horses, or other software failures. A flawed application, if not properly restrained from execution, may affect the other functions of the device and can result in a denial of service attack to the mobile device and even the mobile network.
d) Each flawed application to be revoked is included in a trusted object that may be referred as an Application Revocation List (ARL). The ARL may provide corresponding countermeasures for a given flawed application, for example, to remove it, to replace it with a new version, or simply not to execute it.

User Benefits: The User benefits from an extra line of defence against malware. Even if the User has installed software that contained a virus, worm, or Trojan, the Device may protect critical data, keys etc. and block any functions which depend on such data to operate. Data and keys can be sealed to a certain software state, and are no longer accessible if the malware has changed this software state. For example, the User's own private data would become invisible to the malware.

In a corporate environment, the reliability of a Corporation's applications will be better protected. These applications will usually interact with the Corporation's data and with other corporate applications. Therefore the gain in reliability will be especially important.

Relevant to: Phones and PDAs

Preconditions: The device contains an application which has a list of objects and/or functions it is allowed to access. The device stores an updated ARL.

Success End Condition: The application is used and does only what the user and/or Network Operator and/or Service Provider expects it to do. This means it does not cause any harm to the Device, other applications, the user's account, etc. If the application is revoked, then it will not be able to execute.

Failed End Condition: The attacker makes the application perform malicious actions by violating one of the SW use policies. A flawed application can not be revoked or after it is revoked, it is still executable.

Primary Actors: End user of the device executing the software, and the Device.

Trigger: End user requests software to run.

2.9.2 Lifecycle

Lifecycle stage	Activities undertaken during this stage
Device manufacture and/or initialization	Software use policy is securely provisioned onto the Device when the Device is in an approved state and possibly in a controlled environment.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

Boot time	Integrity of software use policy together with ARL is checked.
Prior to significant runtime activities	Software use policy and ARL are checked and enforced.
Authorised platform upgrade and ARL update	Software use policy is upgraded and ARL is updated in an authorised and controlled manner.

2.9.3 Variations

None listed here.

2.9.4 Threats

1. The application accesses objects for which it does not have rights:
   a) The application obtains unauthorised access to personal data like passwords, payment information etc.
   b) The application obtains unauthorised access tocryptographic keys.

2) The application executes functions for which it does not have rights:
   a) The application calls premium rate numbers.
   b) The application manipulates the user's account.
   c) The application copies itself into another Device.

3) The application revocation can be attacked in the following ways:
   a) One or more records in ARL are deleted so that a failed application is executable.
   b) One or more eligible applications may be maliciously included in ARL so that the user suffers denial of service attack.
   c) ARL is deleted completely.
   d) ARL can be rolled back to an older version so that a recently revoked application is executable.
   e) The verification of the ARL is bypassed before executions. The attacker can do this by (a) not checking the ARL when launching the application; (b) modifying the application identifier to evade being revoked by an ARL.

2.9.4.1 How does the use of TCG specifications mitigate threats?

The TCG techniques allow determination of whether a Device or an application is trusted. Therefore, if an application is restricted to be run only on a trusted platform, the chances of malicious behaviour occurring should be reduced. Furthermore, payment information or passwords can be stored or sealed by the Mobile TPM so that the confidentiality of the data is preserved. Threats 1 (a) and (b) are therefore met.

ARL is a part of security policy either provided by hardware resource or system software security policy. ARL shall be securely updated by the mobile device in a timely fashion. TCG technology can provide platform integrity, especially to insure the security policy including ARL is in place and cannot be removed, as a part of integrity verification. This can be used to counter threats 3 (c) to (e).

The platform integrity will also insure that an ARL is authenticated before used, the threats 3 (a) and (b) can be prevented.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.10 Prove Platform and/or Application Integrity to End User

2.10.1 Characteristic Information

Goal in Context: The end user wants to know whether he can trust his device or an application. This could happen at boot time of the phone, but could also be done when the user starts a sensitive application such as home banking.

User Benefits: The User can easily check or verify at any time that an application or service is trustworthy. If the User's platform loses integrity then the User is quickly warned of this and can contact their Service Provider to gain help.

Relevant to: Phones and PDAs

Preconditions: Device is powered off.

Success End Condition: The device is powered on and an indicator clearly tells the user that the device can be trusted.

Failed End Condition: The attacker modifies the software of the platform. The device is powered on, and though the device should not be trusted the indicator tells the user the contrary.

Primary Actors: End user

Trigger: Power on of device

2.10.2 Lifecycle

Lifecycle stage	Activities undertaken during this stage
Device manufacture and/or initialization	Boot time checks are defined. Reference values for trusted configuration are installed.
Boot time	Platform (or some selected portions of it) integrity is checked and the result is indicated to the user.
Prior to significant runtime activities	Platform (or some selected portions of it) integrity is checked and the result is indicated to the user.
Authorised platform upgrade	Reference values for trusted configuration get updated.

2.10.3 Variations

This use case can be extended to tell the end user whether he can trust the platform and a certain application. This is of particular interest for banking applications (e.g., virtual Visa card) or any applications which require the user to enter passwords or PINs. The user in this case wants a clear (hardware) indication that this application really is the Visa card app and not just a rogue application (for example, a key press logging application) with the same look on the screen as the genuine application.

The use case can also be extended to tell the (U)SIM card (operator) whether it can trust the platform and/or a certain application. This is of particular interest for applications that are distributed between the mobile and the (U)SIM card.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.10.4 Threats

1. If the end user is not explicitly informed about the trust state of the device or an application, he may use an untrusted device or malicious software:
2. An attacker may eavesdrop payment information.
3. An attacker may capture passwords.
4. The application may call expensive numbers.
5. The device transmits personal data of the user.

2.10.4.1 How does the use of TCG specifications mitigate threats?

TCG techniques allow measurement and reporting of the state of the Device as well as the state of an application. This way , information about the Device or application state and whether they can be trusted for a given purpose or not can be provided to the end user and/or to the SIM card.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

2.11 User Data Protection and Privacy

2.11.1 Characteristic Information

Goal in Context: To provide the mobile Device user with the ability to protect their own information from being accessed, viewed, and/or copied by unauthorized entities. This information could include but is not limited to the following types of data:

- Personally identifiable information
- Contact /Address books
- Wallets, credentials, identity tokens

Additionally, the goals is to provide new privacy enhancing capabilities for giving the user access to services and access controlled data or resources in ways which might not require the user to provide personal identity information such as user name and passwords.

For example, a user might purchase the right to access a public wireless network for a specified period of time. Using the TCG specifications the wireless service provider could provide the user's platform with a time based subscription 'token' which allows access to the service. When the user wants to access the wireless network, the token, which is anonymous and does not include any personal identity information, can be used to indicate the right to access the network. In this way, a user would not have to worry about being tracked nor located based on the locations of the wireless networks they are accessing.

User Benefits: TCG specifications can help protect the User against personal data on the Device being released without the User's permission.

Relevant to: Phones, PDAs, and any embedded Device that contains user controlled data.

Preconditions: User must invoke or turn on the use of their specific device provided functions and set the appropriate policies in order to protect their data. These capabilities are 'off' by default until the user authorizes their activatation.

Success End Condition: User controlled data, identity and attestation information is protected from access, viewing, and copying by unauthorized entities.

Failed End Condition: The attacker modifies the SW of the platform to bypass the user protections. The platform integrity checks fail and the Device boots normally.

Primary Actors: End-user, Device, Device Owner, Device Manufacturer, Network Provider.

Trigger: User turns on and sets up protection mechanisms

2.11.1.1 Design Principles

User Opt-in: User related Mobile TPM functions are turned off as the normal condition in new devices. In order for the user related Mobile TPM functions to be enabled the user must turn them on.

Mobile TPM Functions to Support Multiple Ownership Models: The device will provide the capability for multiple entities to have Mobile TPM supplied security functions which can be controlled and applied to only to the data and functions which are authorized to be controlled by each entity.

2.11.2 Lifecycle

Lifecycle stage	Activities undertaken during this stage
Device Manufacturing	Device OEM sets up Mobile TPM functions required to allow each stakeholder, including users, to be able to set passwords and control the Mobile TPM related functions needed to protect and access their specific

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

	data.
User receives new device	User controllable Mobile TPM functions are turned off.
User decides to enable Mobile TPM based functions	User will establish their ownership role over the functions which are available for them to control
User sets policies associated for using their Mobile TPM functions	User provides authentication and then specifies access control and protection policies to be associated with their data.
User Turns off their Mobile TPM functions	User authenticated to the Mobile TPM and subsequently turns off Mobile TPM functions associated with protection of their data

2.11.3 Variations

User Delegation: The user can be specified to be the actual end user, an enterprise, or any other entity which might be delegated to act in behalf of the user's interests.

2.11.4 Threats

1. The users' data is accessible to non-authorized entities.
2. The users' data is available in an unprotected state, either in the device or elsewhere in the network.
3. The users' identity and authentication is compromised, providing access to the security features being used to protect the user data

2.11.4.1 How does the use of equipment that complies with TCG specifications mitigate threats?

The Mobile TPM provides a new and stronger set of mechanisms for creating encryption keys for data protection, but also for applying stronger access control functions to assure that only the authenticated users can access the data.

In addition, TCG technology provides new privacy enabling technology such as use of Attestation Identity Keys with a Privacy Certificate Authority, and Direct Anonymous Attestion to allow the device and user to have access to supporting networks and resources without revealing personally identifiable information, or the platform identity directly.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners