Mobile Trusted Module 2.0 Use Cases

Specification Version 1.0
4-March-2011

Approved

Contact: admin@trustedcomputinggroup.org

TCG Published

TCG

Disclaimers, Notices, and License Terms

Table of Contents

1. INTRODUCTION

Use cases are narratives that define user needs and contexts of use that meet those needs. Use cases are intended to be sufficiently general in that they are not likely to change in their broad scope over time, can serve as generalizations having potential for a variety of more specific usage scenarios associated with them, and hint at the usefulness and value derived from meeting user needs.

The Trusted Computing Group's Mobile Phone Use Cases consider a broad range of usage scenarios where TCG technology, specifically the Mobile Trusted Module (MTM) security technology deemed most appropriate for mobile devices and similar wireless handheld systems with small footprints which require an optimized trusted module, can be applied in the mobile embedded devices context and ecosystem.

This document has been written to guide subsequent technical requirements and specification work within the TCG Mobile Phone Working Group (MPWG). It has been written to provide parties within and outside of TCG with a description of the work being carried out by the MPWG. The usage scenarios outlined herein should illustrate also to Operating System developers what kind of functionalities might be needed to support certain applications that rely on MTM security technology.

1.1 Terms & definitions

Attestation	The procedure of permitting a remote entity to verify the configuration of the proving device (i.e. what software exactly is running on the proving device).
CA	Certificate Authority
CE	Consumer Electronics
CRM	Customer Relationship Management
DM	Device Management
HU	Head Unit: the dash-mounted component in a vehicle which provides a unified information interface for the various components of an electronic media system
IdP	Identity Provider (in conjunction with OpenID)
MFS	Mobile Financial Services
MITM	Man In The Middle [an attack vector]
MNO	Mobile Network Operator
MTM	Mobile Trusted Module
NAC	Network Admission Control
NAP	Network Access Protection
NFC	Near Field Communication
OpenID	Enables end users to use an existing account to sign in to multiple websites

	without needing to create new passwords.
OTA	Over the air
PKCS#11	One of the family of standards called Public-Key Cryptography Standards (PKCS).
POS	Point of sale
Secure Storage	Persistent data storage location where the confidentiality and integrity of data stored therein can be assured
SOC	System on a chip
SSL	Secure Socket Layer
SSO	Single Sign On
TEE	Trusted Execution Environment - a secure area that resides in the main processor or a separate processor of the phone and guarantees that sensitive data is stored, processed and protected in a trusted environment, with the ability to work independently or complementary to a secure element and the standard handset applications.
TNC	Trusted Network Connect

Refer to the TCG Glossary of Technical Terms for additional trusted computing terms and definitions http://www.trustedcomputinggroup.org/developers/glossary

1.2 Actors

In this 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 content protection
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 Trusted Modules for which attestation data may be provided
Device Owner	The legal owner of the Device. The Device Owner is entitled to customise the platform. The owner may be an End User (consumer), an IT Administrator for a Corporation or some other entity
Device Manufacturer	The manufacturer or brand of a Device, typically an Original Equipment Manufacturer (OEM). Also commonly referred to as a Vendor
End User	The ultimate consumer of mobile applications and services, particularly the user for whom the device is designed. The End User may or may not be the Device Owner
Employee	A Corporate worker using a mobile phone to access enterprise applications, data and networks
Service Provider	An entity that wishes to discover properties of a trusted mobile phone platform and provide services to the Device
Mobile Network Operator	An entity that provides cellular communications functionality to the platform
Application Provider	An entity generating and/or selling user applications to be executed on the platform
Attacker	A person or organisation trying to circumvent some policy of the Device, the Service Provider, the Application Provider or the Network Provider
MFS	Mobile Financial Service (such as a bank)

2. USE CASES

2.1 e-Wallet: Mobile Banking

2.1.1 Objective

The objective is to enable the end user to use mobile financial services (e.g. mobile banking) using a HW-secured mobile device such as a mobile phone.

2.1.2 Description

As society becomes more cashless, the likelihood that more end users carry mobile devices than old fashioned cash is increasing. Banking also tends to be a more frequent activity, with growing demand for anytime and anywhere convenience. Therefore mobile banking continues to be an enduring use case.

Security is one of the fundamental elements of any mobile financial service solution, as is usability. The next generation of mobile banking is likely to be very similar to the Internet banking paradigm. It requires an application (either a browser or a standalone application) and an advanced mobile device, such as a modern mobile phone having robust HW-enabled security, an identifiable operating system, and advanced functionality such as enhanced data processing and connectivity.

On the other hand, the banking sector has a very fragmented Internet presence. Nevertheless, there are some commonalities.

- Many financial institutes use TLS or SSL with server side certificates to secure the channel between the banking server and the end users entity
- Most accesses to banking services are browser based, therefore the concern of phishing attacks is quite common
- Many financial institutes utilize one-time-passwords that are mailed to the user or can be deduced from a list of passwords that was provisioned to the user

In addition, some financial institutes consider using user identities provided by governmental organisations. Also, sometimes banking credentials can be utilized directly at some service providers for strong user authentication (via redirect).

A standardised solution for the provisioning protocol would be favourable, so that all banks would provision in the same way (whereby cross-sector consistency would be achieved) e.g. using OMA Device Management Services as part of their solution.

2.1.3 Benefits for Actors

End users avail themselves of mobile banking for everyday consumer banking services, anytime and anywhere. End User benefits are any of the following (not an exhaustive list)

- Account queries
- Transactions (possibly including separate verification/confirmation channel for large transfers)

- Balance and security alerts
- Reminders

Trusted Computing bestows additional end user benefits in mobile banking:

- The overall mobile user experience can be enhanced by the anytime and anywhere convenience of mobile banking.
- Fraud risks are reduced for both End User and Service Provider, as banking data and associated secrets are well protected. Reduced fraud for the Service Provider helps the End User too, through greater diversity of Service Providers supporting mobile banking.
- Privacy and trust is enhanced. The Device may impede interception and eavesdropping of banking transactions.

Mobile financial service providers (such as banks) are interested in extending their services to the mobile space, but without losing control or adding additional expenses for hardware:

- A HW-secured mobile device can validate presented credentials and therefore help in preventing phishing attacks
- There would be no need for paper-slip one-time passwords to be mailed to the user
- Secured automatic provisioning of new one-time password list close to expiry or end of list. Encryption is better than the 'grey envelope' technique
- Utilizing standardized TCG features, the banking services can be secured for a large range of device
- There would be no need for contracts and cooperation with a large range of local operators
- There could be re-usage of the existing financial frontend and backend also for mobile services

Banks may provision the one-time password list to the secure environment for decryption, but they may also provision the algorithms directly, then the one-time password list does not need to be provisioned. That depends on the risk management of the individual bank.

Vendors of mobile devices benefit from being the mobile equipment and user interaction facilitating parts of the value chain to enable mobile banking.

2.1.4 Pre-conditions

The designed solution follows fundamental principles of security (confidentiality, integrity, authentication, non-repudiation and availability). The mobile banking application is deployable onto a mobile device such as a mobile phone. The designed solution can resist both passive and active attacks. The banking application is easy to use (good usability). The OS needs the support of the MTM on one side and on the other side a trusted interface with authorization checking in the application space (in particular the browser).

2.1.5 Post-conditions

2.1.5.1 Success End Condition

An implementation of a mobile banking application (or service) performs to precisely reflect the mobile banking authorisation and transaction as intended by the design.

2.1.5.2 Failure End Condition

An implementation of banking application (or service) is attacked and unauthorised transactions occur.

2.1.6 Lifecycle Scenario

This is just one lifecycle representation amongst probable others.

Lifecycle stage	**Activities undertaken during this stage**
Manufacture / Initialisation	The Device is manufactured with MTM(s) and with the ability to verify the integrity and authorisation of applications. The banking 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 banking application resides on a smart card, then the Device is manufactured with support for a secure path from the MTM to the smart card.
Provisioning / Customization	The end user goes to their web banking portal, authenticates, and then clicks the mobile-enabled service to request the mobile banking service. If the end user is not already a customer of the mobile banking service, certain identification and customer relationship prerequisites are required to be performed. The mobile financial service provider checks, via some challenge-response procedure, the end user's mobile device for service eligibility (presence of MTM and associated vendor information). If device eligibility is verified, the service provider provisions (typically over the air but maybe also via other channels) the mobile banking application (including personalization and activation data) to the device. If application eligibility is verified, provisioning of credentials to the MTM (e.g. certificates, keys, encrypted one-time password list which has no impact on the service backend) is performed.
Use	Each time, the user must authenticate to the mobile banking service (as they must typically do so for all banking transactions). Those parts of the transactions that occur on the client side (in

	the device HW, SW, or on some SOC), whereby sensitive credentials are required to be available to execute the transaction, must occur in a trusted execution environment (TEE), with a secure data channel between the TEE and MTM. The technical security functionality should be hidden from the end user and it should simply function as intended on behalf of the end user.
Management	Management may involve actions such as SW updates. Management functions are required to be authorised by the owner of the MTM and authenticated by mobile device. It should be possible for an implementation to facilitate user data backup and restore. It should be possible for an implementation to facilitate key backup and restore.
Termination	Termination of application use is required when the end user no longer wants to use the device or application. This requires uninstallation of the application and wiping of associated data and credentials, so that mobile banking application and associated information is no longer present or accessible.

2.1.7 Identified Threats

The banking application is attacked to allow an unauthorised transaction.

1. Over-the-air personalisation can be intercepted to duplicate an account in other devices or by other media. It is not assumed that radio protection is always enabled.
2. Confidential information about an account is leaked during transmission. As a result, unauthorised transactions can be made via other devices or media. We exclude the leakage from the server side, since this is out of the sphere of influence of this document.
3. If a user needs to input identity or biometrics to activate a banking transaction, then the identity or biometrics data may be intercepted or leaked via the device. Or this input has been obtained otherwise by an attacker (e.g. by taking a fake fingerprint).
4. For mobile payments that depend on digital signatures for non-repudiation, the private key may be stolen to forge an account owner's signature.
5. A legitimate banking application is installed onto an unauthorised Device.
6. An unauthorised banking application is installed to an authorised Device.
7. Malware gains access to the banking related data (user data, account data).

2.1.8 Threat Mitigation

- TCG technology can enforce platform integrity so that it can help 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 a number of the aforementioned threats.

- A signing key can be created and securely stored using Mobile TPM's protected storage capabilities. This can mitigate threat (4).
- The restriction only to install signed applications and give only those special access mitigates (6) and (7).
- TCG MPWG will not specify the actual protocols and functions but it will specify enablers to allow the robust implementation of these protocols.

2.1.9 Assumptions

It is assumed that trusted computing capability will exist in the mobile financial service´s system and it is outside the scope of this document.

2.2 e-Wallet: Mobile Payment

2.2.1 Objective

The objective is to enable the End User to perform Point Of Sale (POS) payment transactions using a HW-secured mobile device such as a mobile phone.

2.2.2 Description

Security is one of the fundamental elements of any mobile payment solution, as is usability. 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 mobile device. The payment protocol is executed by an application stored at a POS. The involvement of a point of sales into the architecture introduces additional characteristics and legacy. Other forms of mobile payment can be facilitated, such as online subscriptions, online payments, person-to-person value transfer, and vending machines.

A payment with a precise amount must be authorised by the owner of the account and depending on the policy of the financial institute also by the financial institute (e.g. transaction limits, PIN requests etc). The authorisation may be given implicitly or explicitly by the owner.

In case of explicit authorisation, 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, and for this the interface needs to be trustworthy.

The payment transaction might be pre-stored in the device, or in a SOC, and used locally with the POS offline or the transaction may involve online authorization by the bank via the POS.

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.

Mobile Ticketing has similar characteristics as pre-loaded mobile payment transactions. There may be online confirmation with backend infrastructure. There are potentially shadow accounts in the transport backend for recovery purposes, but not necessarily.

Vending machines are also a POS-type of physical payment scenario whereby the POS unit is in effect integral to the dispencing machine.

2.2.3 Benefits for Actors

End users avail themselves of payment method flexibility and obtain reassurance that transactions are performed securely.

Retailers benefit from offering payment method flexibility and security.

The retailer can integrate mobile payment with their loyalty or membership schemes.

The retailer can integrate mobile payment with their customer relationship management (CRM) system to offer more personalized services (e.g. special offers, suggestions based on purchasing behavior) to their customers.

Retailers benefit from operational cost efficiencies by reducing the handling overheads of cash-based transactions.

Mobile financial service providers benefit from being the part of the payment value chain that facilitates end users with a mobile application to conduct mobile payments, and from customisation possibilities.

2.2.4 Pre-conditions

- The designed solution follows fundamental principles of security (confidentiality, integrity, authentication, non-repudiation and availability).
- The mobile payment application is deployable onto a mobile device such as a mobile phone, or onto some SOC.
- The designed solution can resist both passive and active attacks.
- The mobile payment application is easy to use (good usability).

2.2.5 Post-conditions

2.2.5.1 Success End Condition

- An implementation of a mobile payment application performs to precisely reflect the mobile payment authorisation and transaction as intended by the design.

2.2.5.2 Failure End Condition

- An implementation of payment application is attacked and unauthorised transactions occur.

2.2.6 Lifecycle Scenario

This is just one lifecycle representation amongst probable others.

Lifecycle stage	**Activities undertaken during this stage**
Manufacture / Initialisation	The Device is manufactured with MTM(s) and 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. In the case that the payment application resides on a smart card, the financial service provider needs to have some agreed

	cooperation with the smart card issuer i.e. applicable local operator. Also, this may require a specially enhanced mobile smart card to be provisioned; standard 3GPP UICC or SIM cards do not support such a feature. Nevertheless, such cards exist and can be ordered and sent to the user by the operator. The mobile device can be equipped with some contactless technology such as Near Field Communication (NFC).
Provisioning / Customization	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. An application interface to the Trusted Execution Environment is established. Account information is loaded to the payment application over the air from a server. 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 personalisation procedure may happen every time the owner opens a new account with an issuer. The personalisation procedure includes a mutual authentication between the application holder and the server. The confidentiality and integrity of the personalisation procedure is ensured. Provisioning of required data & secrets to the MTM is performed. There is a standardised solution for the provisioning protocol i.e. all banks ideally provision in the same way (cross-sector consistency is achieved).
Use	The end user places their mobile device in very close proximity to a point of sale (POS), or conducts a transaction with an online merchant via the mobile browser. This involves certain authorisation and informative steps via the GUI and storage of transaction receipts to the mobile device. The payment protocol includes an authentication of the account and the server and may include an authorisation of the payment by the owner.
Management	Management may involve actions such as SW updates. Management functions are required to be authorised by the owner of the MTM and authenticated by mobile device. It should be possible for an implementation to facilitate user data backup and restore. It should be possible for an implementation to facilitate key

	backup and restore.
Termination	The payment application is removed from the Device, or else the Device becomes no longer usable with a given payment account by disabling it at the backend. Security data linked to the application or that account are deleted or disabled.

2.2.7 Identified Threats

The payment application is attacked to allow an unauthorised 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 personalisation can be intercepted to duplicate an account in other devices or by other media. The protection of the radio air channel is not assumed.
3. Confidential information about an account is leaked. As a result, unauthorised 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 depend on digital signatures for non-repudiation or integrity, 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 unauthorised Device.

2.2.8 Threat Mitigation

- 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 help 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).
- A signing key can be created and securely stored using Mobile TPM's protected storage capabilities. This can mitigate threat (5).
- TCG MPWG will not specify the actual protocols and functions but it will specify enablers to allow the robust implementation of these protocols.

2.2.9 Assumptions

It is assumed that a trusted computing capability will exist in the retailer´s system and it is outside the scope of this document.

2.3 Strong Mobile Authentication of Enterprise Employees

2.3.1 Objective

The objective is an MTM-facilitated method for seamless and strong authentication of enterprise employees.

Note this use case applies to authentication of enterprise end users, not of the equipment. Thus the focus is different to NAP/NAC/TNC, which deal with authentication of the equipment.

2.3.2 Description

A number of authentication methods facilitated by the MTM are possible depending on intended use and on desired strength of the authentication method.

The end user can get an authentication certificate enrolled and it can then be used for seamless authentication in the background with mobile enterprise PCs, applications and services.

Using an authentication certificate, the end user can get an encryption certificate enrolled, and then use it for reading/encrypting corporate email and documents.

The auth certificate is protected by the device with a PIN which needs to be entered to the device, and the PIN code can be cached for a defined period of time, and optionally this PIN can be tied to the Lock Code of the device for convenience.

The end user can use the certificates in his/her mobile device and connect via Bluetooth/infrared/cable to laptop/PC applications to authenticate or encrypt using the certificates in the mobile device. Once the connection to the other device is broken, no certificates or private keys are left in second device since such credentials never left the mobile device.

Third parties (such as banks) can sign certificates created by device thus enabling standards based strong authentication towards any web service or platform software.

A rather similar use case is assumed to be possible for encrypted email in a mobile device, whereby there is capability to read and respond to encrypted emails (S/MIME).

Enabling certificates on the platform allows email programs to access certificates. With these certificates, the email program can sign or encrypt emails to a recipient whose device has similar encryption capabilities. The email program also uses platform capabilities to verify received signed and/or encrypted emails for digital signature validity.

This use case involves more or less the same actors, pre-conditions, identified threats, threat mitigations, and lifecycle scenario as for strong authentication of enterprise employees, since they share a similar technical foundation.

2.3.3 Benefits for Actors

For the **corporate IT service provider**, there is the efficiency of authentication credentials being provisioned over-the-air (OTA) to the enterprise user's mobile device.

For the **end user**, there is the convenience of having authentication to applications and services done in the background without the need for user interaction, particularly interaction involving security.

The end user avails himself of the mobile device as a strong authentication device; there is no need to carry a separate token or any other corresponding strong authentication gadget.

The end user avails himself of effort-free device access control. When the mobile device moves out of the proximity of the enterprise workstation (laptop, PC, etc.) it locks without user interaction, since the mobile device is used for physical access control. When the end user returns to the workstation, it unlocks without user interaction.

Given proper implementation this could be used outside enterprise solutions, for example a **financial service provider** could issue a certificate to the device allowing strong authentication to the provider's website from the device removing the need for platform specific service provider software or additional one time password solutions. Some banks already use this method for their desktop workstations.

2.3.4 Pre-conditions

- The mobile device provides a secure certificate store.
- Applications are developed to conform with industry standards e.g. PKCS#11.

2.3.5 Post-conditions

2.3.5.1 Success End Condition

- Enterprise user has seamless and strong authentication to their enterprise workstation(s), applications and services.
- The device provides trustworthy certificate store and certificate provisioning mechanism(s).

2.3.5.2 Failure End Condition

- Enterprise authentication is too weak, or unreliable, or too complex, or suffers from poor usability. Trustworthy certificate store or certificate provisioning mechanism(s) is not provided.
- Trustworthy certificate store or certificate provisioning mechanism(s) is not provided.
- If poorly implemented, identity spoofing may be a vulnerability.

2.3.6 Lifecycle Scenario

This is just one lifecycle representation amongst probable others.

Lifecycle stage	**Activities undertaken during this stage**
Manufacture /	MTM(s) and associated trust roots, keys, certificates and policies

Initialisation	may be manufactured into the device (credentials can be provisioned later as well). The mobile device needs to have a complete implementation of PCKS#11, and secure storage (MTM) for private keys. There must be the ability to securely add new trusted third parties post-manufacture.
Provisioning / Customization	The end user uses the device to access the company's certificate provisioning web page (linked to a provisioning server). Depending on companies policies, e.g. if Single Sign On (SSO) is supported, the user authenticates himself and after successful authentication the provisioning server provides the signed certificate to the device MTM without further user interaction. The user is told when process is over. (In this example the company can also be for example a Bank and the user is a customer) The user connects the device to a desktop and starts a program on the desktop which uses company's certificate provision system. After the user has been authenticated the program transfers certificates to the device MTM and the device is ready for use. This scenario can be used with a Service Desk if the company does not allow end users themselves to acquire certificates. In the case of a ServiceDesk or Bank, this could be done this on behalf of the end user; they would authenticate the end user, and then proceed to provision the credentials to the MTM.
Use	A non-exhaustive list of potential usage triggers: 1. Desktop or mobile device Email application using credentials for encrypted (s/MIME) email. 2. Desktop or mobile device VPN application using credentials for strong authentication towards company network. 3. Desktop workstation uses mobile device to authenticate the user allowing access to the workstation. 4. Web server using credentials for strong authentication towards confidential web site. Multiple levels of security are allowed: 1. Maximum level. The user is required to authenticate to the mobile device in each strong authentication attempt 2. Medium level. The user is required to authenticate once to the mobile device when the first strong authentication is complete. This authentication attempt can be cached for a period of time. 3. Lowest level. The user is not required to authenticate to the mobile device, merely having the mobile device works as the second factor.

	Example 1) Accessing a highly confidential company service/server with the mobile device or with a desktop which has connected to the mobile device: Actions required from the user will depend on the security level (1, 2 or 3) set on the device. The end result is that the service can be accessed by the user and the service can be assured that the user accessing the content is the user he claims to be (non-repudiation). Example 2) Accessing highly confidential company email which is encrypted: This can be done with the mobile device or with a desktop which has connected to the mobile device. Actions required from the user when trying to read encrypted email will depend on the security level (1, 2 or 3) set on the device. Example 3) Authorizing actions via signed email: This can be done with the mobile device or with a desktop which has connected to the mobile device. Actions required from the user when trying to send signed email will depend on the security level (1, 2 or 3) set on the device. The receiver can be confident that the authorization has come from the correct person (non-repudiation using digital signature). Authentication certificates may not be recoverable, but encryption certificates may be recoverable, depending on the implementation and usage policy.
Management	Management involves maintenance of the credentials in the MTM and other associated use case data. Certificates can be revoked independently of the device as this is a feature of the Public Key Infrastructure (revocation). Certificates have a validity period and can be updated the same way they are originally provisioned, and can be required to be done periodically (renewal). Optionally, certificates can be renewed using the old certificates as long as they are still valid.
Termination	Revoking the end user's certificates is part of the Public Key Infrastructure and is a normal operation in that environment. The certificates left on the device cannot be used after revocation for further authentication. When certificates' validity period expires, the services associated with their use are no longer accessible. However, they can still be used to decrypt the old messages.

2.3.7 Identified Threats

1. The mobile device is lost or stolen, and malicious user is able to impersonate original owner of the device.
2. A hostile program tries to extract the keys or certificates from the mobile device.

2.3.8 Threat Mitigation

- Provide adequate controls to restrict access to the end user's certificates in secure storage.
- Require a PIN code to activate authentication; mitigates threat 1 as acquiring the device is not enough.
- Perform certificate revocation procedures; mitigates the threat 1 as swift certificate revocation prevents the authentication to be used any further.
- When properly implemented, PCKS#11 and the MTM robustly mitigate threat 2.

2.3.9 Assumptions

It is assumed that a trusted computing capability will exist in the IT service provider´s system and it is outside the scope of this document.

2.4 e-Wallet: e-Health Application

2.4.1 Objective

The objective is to utilize MTM and trusted execution functionality for securely processing the end user's electronic health (e-Health) history which is stored in an e-Wallet on their mobile device. e-The end user's e-Health data can be securely communicated between the e-Wallet, various health services (GP, local clinic, regional hospital, and pharmacy) and virtual health care professionals.

2.4.2 Description

e-Health is defined as the application of technologies (such as mobile communications, the internet and security) in the healthcare industry to improve the access, efficiency, effectiveness, and quality of clinical processes utilised by healthcare organisations, practitioners, patients, and consumers to monitor and improve the health status of patients.

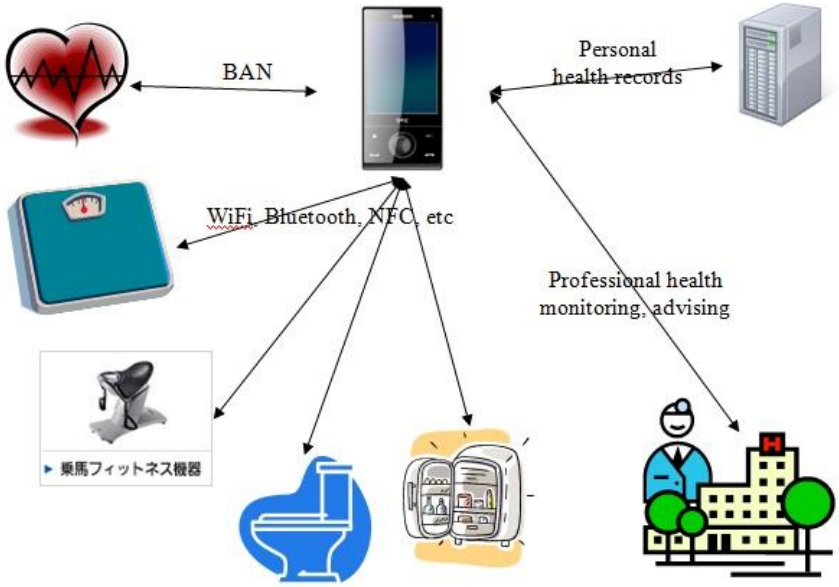

Figure 2.4a

e-Health in this use case refers to an e-Health application carried on the end user's mobile device (e.g. acquired via a dedicated health service URL) which leverages the security services of an MTM and trusted execution environment to process their health records.

The End User's electronic health record is securely stored in the e-Wallet, their health data is securely processed in a trusted execution environment, and communications to health services are attested. These health services may be either or both professional medical facilities and health self-management systems such as cardiovascular disease risk management services.

The e-Wallet can interface with a network of personal Body Area Network sensors to collect, parse, and store and deliver health metrics to authorised destinations for both real-time diagnosis and off-line recording. Furthermore, the e-Wallet can further interface with a network of domestic appliances via WiFi, Bluetooth, NFC and other technologies to gather information about lifestyle choices, such as body weight and fat percentage, exercise frequency, toilet habits, and calorie consumption The interactions with these devices can either be explicit connections on use or batched automatic connections for cases when the e-Wallet device is switched off or otherwise out of range.

The e-Wallet can enable virtual healthcare professionals to collaborate and share information concerning the End User when needed. A copy of the information might be stored at some backend server for disaster recovery or backup purposes. Synchronization with a backend is important for cases such as a flat battery, broken or stolen device, etc.

2.4.3 Benefits for Actors

End User benefits

- End users avail themselves of the convenience of a centralised personal health care repository e.g. for use in telemedicine.
- In health monitoring scenarios (such as for home care patients), the user's ongoing health status can be recorded, monitored, and quickly responded to by healthcare professionals should the need arise.
- Self-management of health is realised by having multiple sources of data gathered together to present the user with an overall picture of their condition.

Health Service benefits

- Health services can securely deliver private health information OTA to patients.
- End User's e-Health data can be scheduled to conveniently synchronise OTA at set intervals with the health centre's or hospital's corresponding computer-based medical records.
- In urgent or emergency situations, healthcare professionals can respond more rapidly by referencing the user's e-Health data for accelerated decision-making.
- Ongoing care monitoring can be automated or delegated to less-skilled staff, and advice delivered on day-to-day non-urgent issues, such as minor straying from a diet or exercise regime or if the end user forgets to take medications, thus reducing costs.

Health Equipment Manufacturers/Suppliers benefits

- Equipment Manufacturers have a defined infrastructure into which to position their products.
- Synergy of equipment and monitoring services provides a market advantage to the Manufacturers.

Health Monitoring Service Provider benefits

- Monitoring Service Providers have a defined infrastructure into which to position their products.
- Synergy of equipment and monitoring services provides a market advantage to the Service Providers.

2.4.4 Pre-conditions

- A patient has a medical condition that does not require admission to hospital, but requires monitoring

2.4.5 Post-conditions

2.4.5.1 Success End Condition

- A patient's health data successfully recorded and secured.

2.4.5.2 Failure End Condition

- A patient's health data is not successfully recorded and secured.
- A data leak occurs.

2.4.6 Lifecycle Scenario

This is just one lifecycle representation amongst probable others.

Lifecycle stage	**Activities undertaken during this stage**
Manufacture / Initialisation	MTM(s) and associated trust roots, keys, certificates and policies are manufactured into the device. The device then has the capacity to provide security services for downloadable applications, such as for e-Health. As the mobile device will be dealing with sensitive personal data, it may be necessary for the MTM to be certified. If so, a certificate describing the protection level (Evaluation Assurance Level, etc) must be installed along with the MTM.
Provisioning / Customization	The health service and end user agree to use e-Health application as a service in the user's e-Wallet. An e-Health application is provisioned to the user's device over some channel (e.g. download URL). The application installs (e.g. run on download), involves sealing and binding certain information to the platform, involves configuration (e.g. counter setup), and involves policies. Note: an MTM API can be a common interface for persistent secure storage of sensitive material like cryptographic keys and credentials.
Personalisation / Use	A trusted state is verified. There is remote attestation between the client mobile device and the e-Health server.

	A Trusted execution environment instance initiated. An e-health application and its configuration is completed and verified. The end user's e-Health profile (for privacy reasons this may be very limited or restricted) is loaded to the e-Health application. There is configuration of authorisation policies to restrict access to particular users, local and remote. The application's tored configuration measurements are compared with expected values, and if all matches OK, the application is ready for use. The e-Health application receives new data (locally from client side and/or remotely from health service), the data is processed in secure environment. There are new configuration measurements (counters initialised etc.) taken and stored. The application usage instance completes. The trusted execution environment instance is completed.
Management	Management involves maintenance of the credentials in the MTM and other associated use case data. Authorisation policies are updated to add new remote users such as health care providers. Similarly, deleting and amending users' credentials may be performed. It should be possible for an implementation to facilitate user data backup and restore. It should be possible for an implementation to facilitate key backup and restore.
Termination	Personal records on third-party servers will be deleted. Personal records on health service databases will be archived according to the prevailing laws.

2.4.7 Identified Threats

1. A compromise of privacy or misuse of sensitive information occurs.

2.4.8 Threat Mitigation

- A robust combination of MTM, TEE, attestation, and PCKS#11 technologies should, in unison, defend robustly against identified threats.

2.4.9 Assumptions

It is assumed that trusted computing capabilities and an enterprise authentication capability will exist in the health service provider´s system and it is outside the scope of this document.

2.5 Media Lending

2.5.1 Objective

The objective is to enable encrypted media to be loaned between mobile devices. There is the bigger picture of a complete content protection-based infrastructure, but at the basic level, this use case is about allowing content encrypted to one device to be played back on another through the use of a loaned key. Even for personal content, the use of encrypted media may be desirable to prevent either accidental or deliberate leakage of the media to a third-party.

2.5.2 Description

The industry is moving toward an all-you-can-consume model, with handsets capable of handling higher quality, and the demand to exchange contents between not just family members but also between friends will surely grow. Given a handset with a standardised MTM and TEE, it becomes possible to support a secure means for implementing a content protection-based system.

A user with a mobile device may stream contents to the device from his home server, having previously registered his device with his home server. He meets up with a friend who also has a media consumption device, and wishes to permit his friend to access the contents on his home server. In thisis scenario, the first user's device will be referred to as the Contents Provider (CP), the first user's home server as the Contents Source (CS), and the second user's device as the Contents Receiver (CR). Note that it is possible that the CP and the CS are the same device, for example if the contents has been previously loaded onto the CP from the CS. Further actors are a Certificate Authority (CA) and an Application Registry (AR) that contains values that characterize Media Player (MP) applications. Both the CA and the AR are well-known to the CP and CR.

The following diagram illustrates the model:

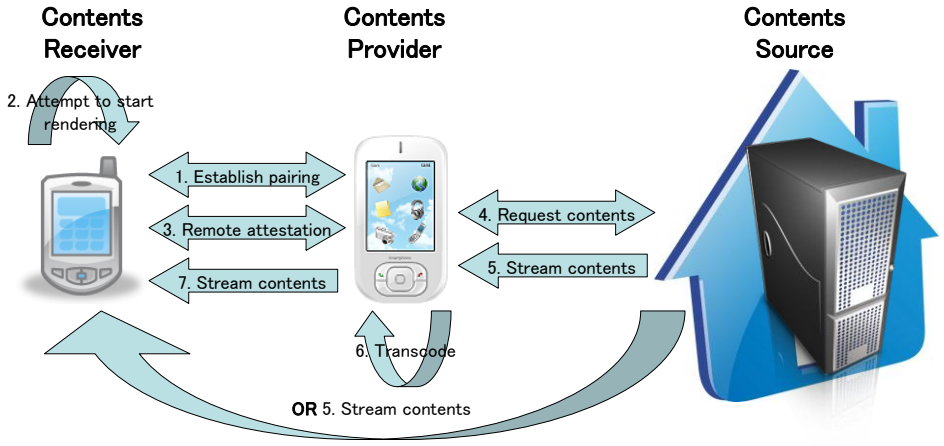

Figure 2.5a

2.5.3 Benefits for Actors

Contents Source Benefits

- Super-distribution of contents.

Contents Provider Benefits

- May lend out media while staying within the law and following the rights granted to the media.

Contents Receiver Benefits

- Easy introduction and access to new content.

2.5.4 Pre-conditions

- Contents Provider has rights to super-distribute or lend the contents.

2.5.5 Post-conditions

2.5.5.1 Success End Condition

- Contents Receiver has correct derivative rights to the contents.

2.5.5.2 Failure End Condition

- Contents Receiver does not have rights, or the wrong rights to the contents.

2.5.6 Lifecycle Scenario

This is just one lifecycle representation amongst probable others.

Lifecycle stage	Activities undertaken during this stage
Initial installation	The CR is provisioned with a media player application that is aware of how to pair with third parties to receive contents and their key material. On installation of the application, the CR creates the necessary key hierarchy to permit pairing and content sharing.
Device pairing	Before the CR can get content from a CS, the CP and the CR perform a pairing operation to obtain an Authorisation Key (AK) and a certificate for it. This AK has associated with it a specific authorization policy to ensure that the media player application can only be used in the expected device environment, and may also have further policies such as the period of validity of the key, or the rights granted to the

	CR regarding editing the content, super-distribution, etc.
Contents rendering	When the CR wishes to render the contents, first the AK is accessed; success in this operation indicates that Secure Boot happened as expected and associated authorisation policy conditions have been satisfied. To initiate the transfer of the contents for either streaming or saving, the CR requests the CP perform remote attestation to verify its state. If the CP is satisfied that the CR is in the correct configuration, the contents may be delivered from the CP to the CR using any suitable standard protocol. The CR can decrypt the stream and render as desired. The process of content rendering itself may involve some further key generation, depending on the actual streaming and broadcasting security protocol used.
Management	If a software player upgrade occurs, the player developer will ensure that all key material can be upgraded as required of the target device.
Termination	On expiry of the key lease all key-related information is deleted from the CR.

2.5.7 Identified Threats

The following assumptions will be made before considering the threats:

1. Both the Contents Source and Contents Provider are robust.
    - Justification: Threats to these devices will be addressed in more fundamental use cases, such as the one of streaming contents to a known device.
2. The Media Player application is robust.
    - Justification: The MTM in particular guarantees a robust environment for executing applications; threats to secure applications will be addressed in more fundamental Use Cases.
3. The Contents Receiver device is a threat even at the time of pairing.
    - Justification: Even though the use case considers the CR device owner to be an associate of the CP owner, the CR device may wittingly or unwittingly be contaminated.
4. The Certificate Authority and Application Registry are robust.
    - Justification: These are key components that by definition should be trusted.
5. The TPM on the Content Receiver device behaves according to specification.
    - Justification: A broken implementation of a TPM will subvert any trusted system.
6. All other implementations of protocols, etc behave according to specification.
    - Justification: A broken implementation of other supporting routines may also subvert a trusted system.

The following threats are present:

- A device with a fake MTM
- A CR having different security properties from CP
- The copying of data from the CR
- Substituting the Media Player for a hacked version on the CR
- A Man In The Middle (MITM) attack between the CR and CP when pairing
- A MITM attack between the CR and CP when rendering

2.5.8 Threat Mitigation

All communication is of course exposed to both eavesdropping and tampering. Denials of Service attacks are also out of scope.

The threats listed above are dealt with as follows:

- A device with fake MTM
  - During the attestation phase, the CP can check the AIK used by the CR with the CA, thus a fake MTM will be detected.
- The CR having different security properties from the CP
  - During the attestation phase, the AIK certificates for both devices may be compared, and based on the EAL of each, the identity of both MTMs, and other information regarding the available algorithms, the CP can make a decision about whether to pair, or what algorithms are best to use in the circumstances.
- The copying of data from the CR
  - Data may be copied, but since it will be encrypted with a content key, the attack is nullified.
- Substituting the Media Player for a hacked version on the CR
  - Secure Boot, or the requirement for a RIM Certificate for launching the application, will prevent the Media Player being launched. Furthermore, at attestation the CP can detect that the expected PCR values are not present.
- A MITM attack between the CR and CP when pairing
  - By using a standard protocol that is immune to MITM attacks, this threat can be countered.
- A MITM attack between the CR and CP when rendering
  - By using a standard protocol that is immune to MITM attacks, this threat can be countered.

2.5.9 Assumptions

The CR creates the pairing root key within the MTM, but the Intermediate Keys are created externally so that the private key can be obtained. However, the data is managed by an MTM object so that it can be protected by the standard mechanisms.

The Authorisation Policy that gets attached to the Attestation Key is implemented using the MTM's Enhanced Authorisation methods.

In theory it is possible to eliminate the Intermediate Keys and replace them by the MTM's TPM2_PolicyAuthorize API, but that weakens the link between the CR and the CP.

2.6 Device Management

2.6.1 Objective

The objective is to monitor, manage, secure and support enterprise mobile devices, for which the MTM can provide security services.

This use case can leverage, as a prerequisite, the use case in this document that describes an MTM facilitated method for seamless and strong authentication of enterprise employees.

2.6.2 Description

Mobile device management is the practice whereby third parties, such as corporate IT departments and MNOs, take responsibility for configuring complex functionality and settings in enterprise users' or subscribers' devices respectively.

Mobile device management has had to evolve in line with increasingly complex mobile devices which have become more difficult to manage. Hence there is a compelling need for corporate IT departments and MNOs to possess the means to manage remote mobile devices efficiently, effectively, securely, and in a standardized way that affords interoperability and scalability.

Typical device management functionality includes (amongst other functionality):

- Mobile credentials provisioning and management
- Firmware updates over the air (FOTA)
- Remote settings configuration
- Data backup and restore
- Remote lock and wipe
- Security updates
- Diagnostics

A number of protocols for device management already exist, amongst them the OMA Device Management protocol specified by the Open Mobile Alliance (OMA).

The MTM could provide security services for the OMA DM protocol.

2.6.3 Benefits for Actors

End users benefit from not having to worry about complex device configuration and management.

Mobile device management third parties benefit from the operational efficiencies and effectiveness afforded by being able to proactively and systematically configure and manage many hundreds or thousands of remote mobile devices.

Mobile vendors benefit from the technological advances in meeting the device management expectations and requirements of end users.

2.6.4 Pre-conditions

- The device management third party has the protocols, procedures and policies established to facilitate remote mobile device management.

2.6.5 Post-conditions

2.6.5.1 Success End Condition

- Mobile device management is securely accomplished by the responsible third party, without negatively impinging the mobile device usability and user experience.

2.6.5.2 Failure End Condition

- Mobile device management fails, or the security involves fails, or the mobile device usability and user experience is negatively impinged.

2.6.6 Lifecycle Scenario

This is just one lifecycle representation amongst probable others.

Lifecycle stage	**Activities undertaken during this stage**
Manufacture / Initialisation	MTM(s) and associated trust roots, keys, certificates and policies may be manufactured into the device (credentials can be provisioned later as well). The mobile device needs to have a complete implementation of PCKS#11, and secure storage (MTM) for private keys. There must be the ability to securely add new trusted third parties post-manufacture.
Provisioning / Customization	The first instance of device management configuration is performed by corporate IT or the NMO prior to the end user receiving the mobile device, or done after the user has started using the device. Communication is asynchronously initiated by the device management server whereby the server sends a challenge to the mobile device. The challenge-response handshake and subsequent processing occurs in the TEE using device authentication data stored in the MTM, and data from the device management server such as enrolment certificates are securely stored to the MTM. This is the first device management configuration that enables and disables device features, and changes device settings and parameters.
Use	Subsequent device management handshakes and data processing occurs in a similar fashion, leveraging the security functions of the MTM and the TEE.
Management	Management involves maintenance of the credentials in the MTM and other associated use case data.

	Device management-associated certificates can be revoked independently of the device as this is a feature of the Public Key Infrastructure (revocation). Device management-associated certificates may have a validity period and can be updated the same way they are originally provisioned, and can be required to be done periodically (renewal). Optionally, certificates can be renewed using the old certificates as long as they are still valid.
Termination	Revoking the end user's certificates is part of the Public Key Infrastructure and is a normal operation in that environment. The certificates left on the device cannot be used after revocation for further authentication. When certificates' validity period expires, the device management services associated with their use are no longer accessible.

2.6.7 Identified Threats

1. The mobile device is lost or stolen, and a malicious user is able to impersonate the original owner of the device e.g. in order to access enterprise data.
2. A hostile program tries to extract device management keys or certificates from the mobile device.

2.6.8 Threat Mitigation

- Provide adequate controls to restrict access to the end user's certificates in secure storage.
- Perform certificate revocation after some predefined number of failed attempts to access device management keys or certificates are detected.

2.6.9 Assumptions

It is assumed that a trusted computing capability will exist in the IT service provider´s system and it is outside the scope of this document.

2.7 Identity Management

2.7.1 Objective

The objective is to enable the End User to utilize SSO (Single Sign-On) or OpenID features using a hardware-secured mobile device such as a mobile phone.

2.7.2 Description

The end user can acquire a certificate from an identity provider (IdP) which is compatible with OpenID. The certificate can cover both the identity provider's asymmetric public key and the end user's asymmetric public key which is generated and stored in MTM.

A MTM-embedded HW-secured phone can access the relying party's site (e.g. a provider's service), and when the relying party requests an OpenID, then the HW-secured phone executes a remote authentication with the relying party whereby the identity provider will be the CA.

An IdP will issue a certificate through enrolment of personal data by the HW-secured mobile phone user. The secure certificate enrolment phase is not outlined here and may rely on a pre-shared secret, e.g. using the existing UICC secret. The IdP also responds to the relying party's authentication requests.

The user uses their mobile phone browser and is redirected by the relying party to the OpenID IdP. If asymmetric authentication is used, then the IdP needs to send some form of nonce or token to the MTM via the browser (the usage of a nonce/token is to avoid replay attacks). The MTM needs to validate and authorize the request from the browser to counteract malicious scripting attacks. Then it can sign the nonce or token and include in the signed response potentially also other data, e.g. phone identity data (e.g. device ID), application specific requested data, and identity provider-requested specific data and random numbers, for dynamic data authentication. This signed data is then returned via the browser to the IdP. It should be noted that this certificate-based authentication at the IdP requires from the OpenID IdP a PKI infrastructure and assumes prior user-certificate enrolment.

Some potential triggers are as follows:

- The mobile device incorporates secure elements such a MTM.
- Web access data loads done by mobile phone increase rapidly and mobile device end users are reluctant to type ids and passwords by the touchpad displayed in phone screen.

2.7.3 Benefits for Actors

The mobile device owner can access services with one enrolment to an identity provider's CA service, without any provisioning of personal data.

The mobile device owner doesn't need to provide their own personal data to the identity provider, because the entire enrolment procedure is processed by a HW-secured MTM.

The MTM provides application integrity checks to ensure a TEE.

No malicious attacks can hijack certificates, nor conduct phishing.

2.7.4 Pre-conditions

- A TEE is mandatory between the MTM and middleware.

2.7.5 Post-conditions

2.7.5.1 Success End Condition

- An implementation of identity management is used instead of remote authentication and dynamic data authentication.

2.7.5.2 Failure End Condition

- The mobile device is attacked by malware or there is a successful phishing attack.

2.7.6 Lifecycle Scenario

This is just one lifecycle representation amongst probable others.

Lifecycle stage	**Activities undertaken during this stage**
Manufacturer / Initialization	The device is manufactured with a MTM and with the ability to provide remote authentication with a website which provides SSO or OpenID to achieve authentication or acquire a certificate. To do this, the MTM provides a secure application to perform remote authentication and also NVM storage to store OpenID/SSO information. The MTM also should provide remote update of validity of OpenID/SSO information in MTM during the authentication phase.
Provisioning / Enrolment	The end user uses the device to access a website/server which provides OpenID/SSO services.
Updates	The certificate has a limited lifespan, and is also invalidated or revoked after some preset number of failed attempts. Some websites' policy might request re-creation of certificate.
Termination	The end user chooses to discard/unsubscribe their OpenID/SSO registration and the stored credentials are deleted/wiped. A website/server can terminate the end user's OpenID/SSO service. A website/server can request a fee to enroll/extend an OpenID/SSO service.

2.7.7 Identified threats

1. The device is lost or stolen.
2. Malware attacks the execution environment of HW-secured mobile devices.
3. Security: exposure of meta-information in a URL.

2.7.8 Threat mitigation

- Strong authentication is provided by Identity provider (IdP).
- There is differentiation of authentication process for register, login, and logout.
- Physical presence for validating the End User is applied.

2.7.9 Assumptions

- There exists MTM-enabled OpenID standardization which includes certain types of keys, a procedure for remote authentication, methods of signing signatures, and capacity in the MTM for identity management.
- An Identity provider provides a CA service which enables a MTM to perform a secure authentication process.

2.8 Vending Machines with Trusted Execution Environment

2.8.1 Objective

The objective is to utilize MTM security functions in vending machines.

Vending machines are now quite advanced terminals, able to report home when stock levels get low and to receive information such as news and weather to display on built-in screens. Furthermore, electronic payment options, whether it be SMS call-backs or RFID-based, may also require a link to process these sales.

Although a vending machine is hardly a portable device, the requirements for Secure Boot, trusted execution and cellular communications bring such machines within the scope of the Mobile Phone Working Group.

The provision of such a secure environment is the objective of this use case.

2.8.2 Description

The physical security of vending devices is of course a well-known problem, but as these devices get more sophisticated, the scope for attacking their security integrity, for example via electronic attacks, widens.

In addition, with RFID-based payment systems, the back-end settlement service provider may require a minimum level of security within the software and hardware.

Although from the average consumer's point of view this security will most likely be invisible and perhaps even incomprehensible, with a device certified to a standardised Protection Profile, the reliability of the vending machine can be demonstrated to interested technically-proficient press, and thus such merits will filter down to the consumer level.

Figure 2.8a illustrates a vending scenario.

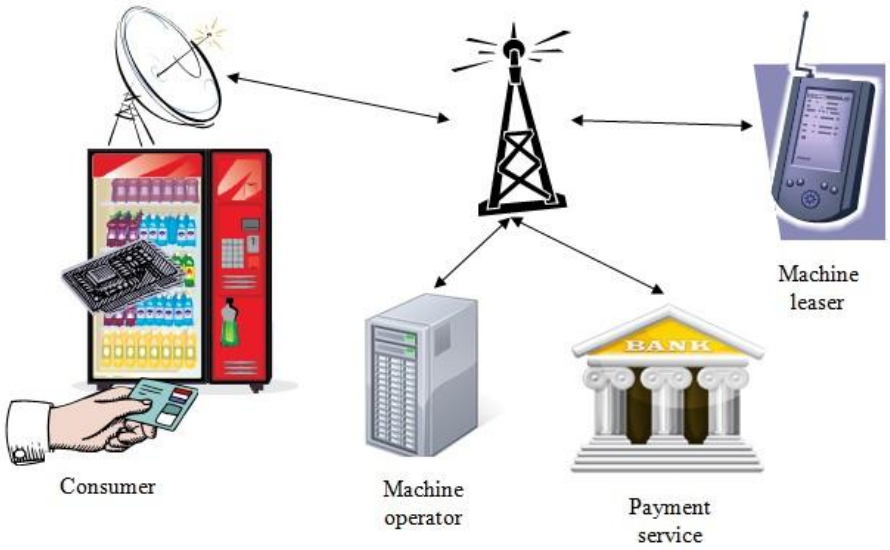

Figure 2.8a

A vending machine is equipped with a communications module that provides a two-way link to the machine operator for passing information such stocking levels and device faults, the machine leaser for passing information such as sales levels and pricing information, and a financial institution that handles card-based payments such as for electronic cash through NFC or traditional magnetic strip. In the case of the mobile network being down, the vending machine's trusted execution environment (TEE) is able to cache information until such time as service is restored or the machine operator manually recovers data by an in-person visit to the vending machine.

2.8.3 Benefits for Actors

Machine Operator Benefits

- The TEE application allows optimal carrier to be selected and changed remotely as desired
- Vending Machine stock level information, helps operator to make decisions on pricing, product selection, etc

Machine Leaser Benefits

- A trusted execution environment enables secure electronic payment
- Vending Machine stock level information the helps leaser to make decisions or advise operator on pricing, product selection, etc

Consumer Benefits

- The vending machine offers multiple payment methods

Payment Service Benefits

- As transactions can be verified online, better protection against fraud
- More payment options available means more transaction service charges

2.8.4 Pre-conditions

- The TEE must be non-removable.

2.8.5 Post-conditions

2.8.5.1 Success End Condition

- Goods are sold at the appropriate price and reported over the M2M network.

2.8.5.2 Failure End Condition

- Goods are sold incorrectly, or the M2M network is not correctly configured.

2.8.6 Lifecycle Scenario

This is just one lifecycle representation amongst probable others.

Lifecycle stage	**Activities undertaken during this stage**
Manufacture	The trusted execution environment is prepared and initialised with no carrier configured.
Device installation	During physical installation the trusted execution environment and other trusted components need only perform diagnostic self-checks.
Personalisation	This may be carried out locally on the device or remotely via the cellular network in a manner that does not require the presence of an activated trusted execution environment. Device personalisation configures the MCIM component with a selected carrier identifier, and then personalisation of the vending machine, including identifying the device leaser. This operation may be performed as often as required, including the deletion of any or all of the personalities within the trusted execution environment. The general credential provisioning could utilize protocols like 3GPP TR 33.812.
Configuration	The contents to be vended are selected and priced as required. This operation may be performed as often as required.
Stocking	Stocking levels are reported to both the machine operator and the machine leaser.
Vending	If the customer chooses to pay by credit, the inserted or scanned card may be verified with the credit company. If the card is refused or the network is not accessible, the vending transaction is cancelled. On a sale, reports are delivered to both the machine operator and the machine leaser. If the network is down, transactions are cached. For a credit or debit card sale, reports are delivered to the credit company.
Management	If the mobile network is down, the machine operator, or if permission has been delegated the machine leaser, may pay an in-person visit to the vending machine to manually perform any pending transactions. A device equipped with an MTM (or TPM) and a working communications module may be used as a communications proxy, or else the pending data may be downloaded in an encrypted form to be processed at a separate location.
Termination	A mobile device's relationship with a vending machine may be terminated at the request of the device owner or at the request of the vending machine owner. All key material and associated information on the vending machine and shared with the mobile device will be deleted by the vending machine on receipt of an authorised and authenticated deletion command.

2.8.7 Identified Threats

The following threats apply to the vending machine electronic components; the physical security of the vending machine itself is out of scope, even though physical attacks may be detected and reported via the electronic components.

1. A stolen credit card is used for payment
2. There is eavesdropping, tampering or jamming the communications from the device to prevent payment processing
3. A bogus operator transmits incorrect or malicious commands to the device to perform DOS
4. A bogus operator transmits incorrect information to the device to re-price goods for sale
5. An operator tampers with reporting software to report incorrect sales details to leaser
6. There is removal of the TEE and use of it for personal connectivity.

2.8.8 Threat Mitigation

- By using the trusted execution environment interface to access the card issuer, threat [1] can be countered. Furthermore, the card issuer can attest to the device to verify that it is allowed to request card verification, and further query the device to obtain location information, or even a photograph of the user as needed.
- A standard encrypted protocol (SSL, etc) will prevent eavesdropping and tampering in [2]. Furthermore, all protocol-handling modules should be tested with fuzzing software to ensure robustness. Jamming is unavoidable, but the device should have sufficient protected non-volatile storage so that it can cache unprocessed payments. The device may have a limit (in terms of either or both time since last successful online update and money) for how many transactions it should cache before disallowing further electronic payments.
- A standard encrypted protocol will also block threat [3] and [4]. Full testing of the protocol with fuzzing tools will further serve to secure the interface from malformed commands.
- Assuming the leaser trusts the device manufacturer (a fair assumption), then to mitigate threat [5] the manufacturer will publish expected attestation information and an attestation key certificate, enabling the leaser to confirm that the correct software is present on the device.
- For [6], the exact method for switching vending machines into free mode is unknown (is it a local vibration sensor, a cellular broadcast, or a radio signal?) thus currently it is impossible to say how to mitigate it.
- For [7] the TEE should be firmly embedded into the vending hardware and be a non-removable element.

2.8.9 Assumptions

The machine may be manufactured with a machine operator identity embedded within it, or at least some form of master identification that can securely assign a machine operator identity, preferably at the time of manufacture or before being shipped out of the

manufacturer's facilities. This enables the physical installation of the device to be conducted without direct interaction with the machine manufacturer or machine operator.

To personalise the device, first the machine manufacturer acts as an intermediary to introduce the machine operator to the device, then the machine operator can perform a similar role to introduce the machine leaser to the machine. However, the machine leaser may not necessarily do the personalisation directly, so either the operator or leaser can perform the personalisation role. Furthermore, there needs to be a set of rights associated with such factors as controlling pricing and the loading of the machine.

Within MTM v2.0 this may be achieved by using EA Policies to control which actors can access encryption keys; the machine operator will be the MTM Owner. The device personalization by the communication provider can also be done via an intermediate entity (see 3GPP TR 33.812, Alternative 1). It should be noted that, during manufacture, it will not be known to which network the device will actually connect to. On the other hand, the communication network provider wants to have assurance, that he provisions the communication network access credentials to a device belonging to an authorized subscriber (vending machine operator) i.e. properly paying customer.

Furthermore, all the leaser's communication with the machine needs to be monitored and vetted by the operator, both automatically (such as no loading Coke™ into a Pepsi™ machine) and manually (such as contacting the operator if suspicious pricing is set) as the need arises. By ensuring that all keys for communication between the leaser and the machine have the MTM Owner as part of the EA Policy chain, the operator can easily gain access to the leaser's communications. By adding features to the TSS or Abstraction Layer, MTM Owner-specific policies may be transparently added to the EA Policy for new objects. Alternatively, if EA Policy Modification is supported, after creation the MTM Owner can add its own specific policies to keys.

Protecting the integrity of reports of sales to the machine leaser is important because as mentioned above the MTM Owner (machine operator) can access the machine leaser's keys. However, this integrity may be easily provable by having the machine sign all reports with an attestation key that the leaser can access to prove to himself that the MTM within the machine has actually signed the report.

Financial reporting of card and electronic cash sales may be handled is a similar fashion, although the financial institutions may require that the machine owner does not retain the ability to access any keys within the device.

2.9 Application Store

2.9.1 Objective

The objective is for the end user to benefit from the utilization of MTM security functionality during application store transactions. The end user navigates to an online application store, purchases, downloads and installs chosen software applications, with confidence that the transaction has been conducted securely.

2.9.2 Description

An application store, a concept originated from the concept of value-added services (VAS), is an online service for mobile devices which allows end users to browse, select and download purchased (and freebie) applications from the service. The applications, which are commonly mobile games, utilities, novelties, ringtones, screensavers, and wallpapers, can be typically downloaded directly onto the target device (such as a mobile phone or tablet device).

Application store software products are typically digitally signed after a vetting procedure confirms suitability for distribution. The digital signature is a tamper-evident seal that provides some degree of accountability of who wrote the particular application.

However, digital signatures don't guard against all security woes, since they only provide some information about the content itself. Transaction tunnel security, a trusted execution environment, secure storage for sensitive client-side credentials, as well as service-side data security, are still required infrastructure via which digitally signed content can be conveyed securely from the application store to end users.

Application stores require a robust end-to-end security paradigm which enables a secure, consistent and positive developer experience, and a secure, consistent and positive user experience which reinforces user loyalty, customer retention, and attracts new customers.

2.9.3 Benefits for Actors

End users benefit from additional usefulness of their mobile device facilitated by a wide choice of compatible after-sales firmware and third-party content.

Vendors benefit from the added appeal of their mobile devices when supporting after-sales firmware and third-party content.

Application store owners benefit from the positive effects of offering their customers value-added services, and by integrating applications management, billing, and CRM

Vendors, as well as being device manufacturers, can also be application store owners.

Content developers benefit from the positive effects of promoting their third party software products.

Mobile network operators benefit from the positive effects of network traffic. MNOs, as well as being a provider of services for mobile phone subscribers, can also be application store owners.

2.9.4 Pre-conditions

- The mobile device has a MTM, a TEE, PKCS#11, and is set up with an application store account.

2.9.5 Post-conditions

2.9.5.1 Success End Condition

- The end user effortlessly and confidently installs a trustworthy application from an application store via a secure end-to-end transaction tunnel, without any exposure of sensitive personal data, store account data, or transaction payment data.

2.9.5.2 Failure End Condition

- The end user's sensitive personal data, or store account data, or transaction payment data is either knowingly or unknowingly exposed during an application store transaction.

2.9.6 Lifecycle Scenario

This is just one lifecycle representation amongst probable others.

Lifecycle stage	**Activities undertaken during this stage**
Manufacture / Initialisation	The mobile device comes equipped with a MTM, a TEE, and application store access via a download link or a mobile web browser.
Provisioning / Customization	The end user creates an account with the application store. Involves PKCS#11 key exchange and user certification enrolment, account setup data, using user and device identity credentials stored in the MTM, and using the TEE as the processing environment. For enhanced end user experience, successive accesses to the application store may be expedited once the initial handshake setup procedure is successfully concluded.
Use	The end user downloads some application from the application store. Involves a client-server handshake using MTM credentials, the TEE for execution, and content delivery via a secure tunnel, using the already established user account stored at the backend to process the transaction payment.
Management	Management involves maintenance of the credentials in the MTM and other associated use case data. Certificates can be revoked independently of the device as this is a

	feature of the Public Key Infrastructure (revocation). Certificates have a validity period and can be updated the same way they are originally provisioned, and can be required to be done periodically (renewal). Optionally, certificates can be renewed using the old certificates as long as they are still valid.
Termination	Revoking the end user's certificates is part of the Public Key Infrastructure and is a normal operation in that environment. The certificates left on the device cannot be used after revocation for further authentication. When certificates' validity period expires, the services associated with their use are no longer accessible. However, they can still be used to decrypt and use older content.

2.9.7 Identified Threats

1. Malicious or flawed applications may slip through to end users' devices if there is inadequate vetting of application candidates, or inadequate store web site security.
2. The end user's sensitive personal data, store account data, or transaction payment data may be susceptible to eavesdropping and MITM attacks if there is inadequate transaction tunnel security, i.e. there are plaintext data transmissions.
3. End-to-end transaction security fails if client-side authentication is unreliable, or if the transaction tunnel is vulnerable, or if server-side authentication is unreliable, i.e. the chain of trust is broken if just one link fails.

2.9.8 Threat Mitigation

- Client-side sensitive credentials are stored in the MTM.
- Client-side transaction processing is conducted in the TEE.
- Applications are downloaded directly to the requesting mobile device, i.e. there are no interim holding locations which may be vulnerable.
- All flows of transaction data occur in a secure tunnel between the client device and the store server, i.e. all transactions are encrypted.

2.9.9 Assumptions

- The end user can access an application store either via a download link or mobile browser in their mobile device.

- The application store has a security policy available for developers and end users.

2.10 Device Interconnectivity in Vehicles

2.10.1 Objective

The objective is to integrate a mobile device and a head-unit (HU, the dash-mounted component in a vehicle which provides a unified information interface for the various components of an electronic media system) using trusted computing technology, whereby the control and interaction of applications and services running on the mobile device will be securely and seamlessly replicated in the car environment.

2.10.2 Description

The secure connectivity and interoperability of devices in vehicle environments can be afforded by the use of trusted computing MTM technology to enable devices and vehicle HUs to authenticate each other and then interoperate seamlessly and securely.

For example, the HU can verify that the communicating mobile device is a compliant or approved device (device attestation).

Some specific software program at the other end of the communication channel can likewise be authorized (software attestation).

Appropriately labeled data in the mobile device can ensure that the HU presents only appropriate content to the driver based on the vehicle's context, e.g. no video content would be displayed to the driver when the vehicle is moving.

Such attestation requires a pre-established trust relationship between the HU device and the mobile device.

At their respective manufacture times, each device is provisioned with a key pair and authorized manufacturer certificates.

Attestation, and related key and certificate, operations occur in the Trusted Execution Environment (TEE).

Device certificates (issued by the device manufacturer /vendor) can have extensions or certificate policy statements to indicate the strength (aka security level) of attestation.

Benefits for Actors

- For the **end user**, the complexity of setting up device interoperability in vehicle environments (where distractions can be dangerous) can be significantly reduced. Services and content in the end user's mobile device can be seamlessly and securely integrated with vehicle speakers, displays and control systems. The end user avails themselves of the dependability and reliability of a robust security implementation against threats such as bluejacking of the HU and mobile devices in the vehicle environment.

- For the **mobile device manufacturer**, their mobile products become acceptable for safe use in an automotive environment, thereby expanding the mobile products' variety of usage environments.
- For the **automotive manufacturer**, safe and secure interoperability with mobile devices such as phones and tablets becomes an evolutionary and marketing advantage.

2.10.3 Pre-conditions

- The vehicle manufacturer has implemented trusted computing technology into their products.

2.10.4 Post-conditions

2.10.4.1 Success End Condition

- An implementation of attestation and interoperability between communicating devices in vehicle environments functions securely and seamlessly as intended.

2.10.4.2 Failure End Condition

- An implementation of attestation and interoperability between communicating devices in vehicle environments becomes compromised, or, malicious software successfully masquerades as being legitimate.

2.10.5 Lifecycle Scenario

This is just one lifecycle representation amongst probable others.

Lifecycle stage	**Activities undertaken during this stage**
Manufacture	The mobile device and vehicle HU are manufactured each with an MTM. Required keys and associated certificates are provisioned into the mobile device and HU.
Use	For initial pairing, some channel such as Bluetooth or USB is used to bind/pair the mobile device and HU. Port binding may be enough; the OS on the mobile device prevents other components from binding to the same port as long as the attested component holds the port. Once the (TCP) connection breaks, the HU should trigger a new attestation. For attestation between the mobile device and the HU, the HU device sends identifier of the software component that should be attested. A random nonce is included for replay-protection. A trusted software component within the mobile device measures the requested component. If the measurement matches the expected/approved value (in a RIM

	cert), a pre-defined value (including an IP address and port) is extended into a platform configuration register (PCR) that is reserved for this use. The mobile device performs a TPM_Quote operation that signs the PCR content. A nonce is included with the signature. The mobile device sends back the resulting signature, the previous PCR value (for simple verification) and the certificates. The HU verifies the quote signature and saves the IP address and port. The HU attests the type of content it receives from the mobile device and the type of application that sends the content.
Management	Management involves maintenance of the credentials in the MTM and other associated use case data. The mobile device may acquire a software update which requires the HU to likewise modify or replace its software, and this may involve attestation, revocation and replacement of certain credentials.
Termination	Any key material and information in the HU associated with the mobile device is deleted/wiped by the HU on receipt of an authorised and authenticated deletion/wipe trigger.

2.10.6 Identified Threats

1. Malware masquerades as the attested software component.
2. The mobile device and HU communication is intercepted and there is some consequent compromise of privacy.

2.10.7 Threat Mitigation

- Strong authentication.
- Physical presence of the end user i.e. the vehicle operator.

2.10.8 Assumptions

It is assumed, apart from standardised trusted computing using the MTM in an automotive setting, that the device interconnectivity procedure and usability would become standardised across the automotive industry.

It is assumed similar trusted computing techniques can be applied to in the automotive content, such as:

- Mandatory alco-lock protection and override prevention,
- Vehicle software identity update protection,
- Protected storage of and access to the Vehicle Identification Number (VIN).