OMTP PUBLISHED

OMTP

APPLICATION SECURITY FRAMEWORK

Version:	2.2
Status:	Approved for publication
Date of Publication	6th June 2008
Owner:	OMTP Limited

CONTENTS

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

The information contained in this document represents the current view held by OMTP Limited on the issues discussed as of the date of publication.

This document is provided “as is” with no warranties whatsoever including any warranty of merchantability, non-infringement, or fitness for any particular purpose. All liability (including liability for infringement of any property rights) relating to the use of information in this document is disclaimed. No license, express or implied, to any intellectual property rights are granted herein.

This document is distributed for informational purposes only and is subject to change without notice. Readers should not design products based solely on this document.

Each Open Mobile Terminal Platform member and participant has agreed to use reasonable endeavours to inform the Open Mobile Terminal Platform in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. The declared Essential IPR is publicly available to members and participants of the Open Mobile Terminal Platform and may be found on the “OMTP IPR Declarations” list at the OMTP team room.

The Open Mobile Terminal Platform has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions.

Defined terms and applicable rules above are set forth in the Schedule to the Open Mobile Terminal Platform Member and Participation Annex Form.

© 2008 Open Mobile Terminal Platform Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited. “OMTP” is a registered trademark. Other product or company names mentioned herein may be the trademarks of their respective owners.

1 INTRODUCTION

The proportion of Terminals providing open platform functionality is expected to continue to increase moving forward. The openness of these platforms offers significant opportunities to all parts of the mobile eco-system by delivering the ability for flexible programmes and service delivery options that may be installed, removed or refreshed multiple times in line with the user's needs and requirements. However, with openness comes responsibility. Unrestricted access to mobile resources and APIs by Applications of unknown or untrusted origin could result in damage to the user, the Terminal, the network or all of these, if not managed by suitable security architectures and network precautions.

Certification of Applications by Approved Authorities provides a mechanism to assure the Terminal of the trustworthiness of an Application. This document relies upon the fact that certification schemes exist which can be used to sign Applications. This allows the Terminal to check whether the Application has been approved and if so, by which scheme, and for what levels of access to functions. See 'Mobile Application Security: Requirements for Mobile Applications Signing Schemes' [1] for more details.

For an effective solution, it is necessary to carefully balance the security needs of operators, Manufacturers, developers, enterprises and users.

1.1 DOCUMENT PURPOSE

The purpose of this document is to define a framework which identifies the key functional groups presented on the Terminal which may be abused by rogue or badly written Applications[1]. These functional groups are then mapped against a set of Trust Levels (also known as tiers, domains or levels of assurance) which correspond to the level of trust which OMTP place in that Application via an appropriate signing scheme. This mapping will indicate whether an Application may have access to that functional group. Whether the Application can make use of the function or a particular API contained within that functional group may depend on whether it has been granted access through the certification process and also upon other measures such as operator or user settings and user prompting.

An Application which has been written by an anonymous developer and had no testing performed upon it will have a very low level of trust associated with it. This low trust need not prevent the Application from being installed upon a Terminal, but access to some functional groups will be restricted (by user prompt) or barred for that Application.

[1] As input work for this ASF work, the OMTP Security Work group has collected and described use cases and attack scenarios which may exploit this open access if not adequately addressed by phone architecture or network precautions and process.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

Each Trust Level is assigned a set of functional groups which will be the maximum allowed for that level of trust. Grant will normally be for a subset of the functional groups within a given level, the subset consisting of only those functional groups declared by the Application. Further protection from Malware attacks may be provided by ensuring no grant is made for functional groups within the level that are not declared by the Application.

1.2 INTENDED AUDIENCE

This document is targeted at operators, Manufacturers and also to certification scheme authorities. This document will however, also be of use to developers to understand access conditions, prompting regimes and the benefits of Application certification.

1.3 PREREQUISITES

As stated above this document bases its security architecture on a number of levels of trust that involve granting access to defined functional groups. Trust Levels are bound to Applications by the use of authorised Public Key Infrastructure certification processes.

Prerequisites for Terminals are:

- Terminals must support a security scheme based on a number of Trust Levels.
- Terminals must support a set of distinct functional groups.
- Terminals must support run-time prompts provided by the Application Execution Environment (AEE)

The certification of Applications can be done by different parties such as operators, Manufacturers or third parties. A number of third party certification schemes have already been established and are therefore considered as important elements of this security framework. These include:

CERTIFICATION SCHEME	OPERATING SYSTEM/ EXECUTION ENVIRONMENT	COMPANY RUNNING SCHEME
Java Verified™[2]	Java(TM) Platform, Micro Edition	Sun
Mobile2Market[3]	Windows Mobile	Microsoft
Symbian Signed[4]	Symbian OS	Symbian

[2] JVP: www.javaverified.com

[3] M2M: http://msdn2.microsoft.com/en-gb/windowsmobile/Bb250551.aspx

[4] Symbian Signed: www.symbiansigned.com

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

CERTIFICATION SCHEME	OPERATING SYSTEM/ EXECUTION ENVIRONMENT	COMPANY RUNNING SCHEME
TRUE BREW[5]	BREW	Qualcomm

Other schemes may be added to this list subject to follow up work within OMTP.

1.4 REQUIREMENT LEVELS

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC2119 [2].

- MUST: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- MUST NOT: This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
- SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- MAY: This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides).

The requirements within this document are uniquely identified using the following format:

ASF -####(.#.#), where:

[5] BREW: http://brew.qualcomm.com/brew/en/developer/commercialization/application_testing.html

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

- ASF stands for Application Security Framework
- #### is a 4 digit number uniquely identifying the recommendation
- (.#.#) are numbers that identify sub-recommendations

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

2 SENSITIVE FUNCTIONAL GROUPS

This section categorises the key functional groups of the Terminal which could be used or abused by Applications executing on the Terminal. Applications with limited trust (i.e. those where the Terminal cannot identify the source of the Application) shall be prevented from accessing certain of these functional groups (see also section 3 Trust Levels).

REQ. ID	RECOMMENDATION
ASF-0010	Where a Terminal implements a function described in the sections 2.1 to 2.17, this function SHALL be allocated to the appropriate functional group with behaviour as stated.

More than one function may be mapped to a functional group.

2.1 CIRCUIT SWITCHED CONNECTIONS

Functions accessing the core telephony function, i.e. by either initiating an outgoing voice call or responding to an incoming call, including supplementary service requests. Both voice and circuit switched data calls are included. This group includes access via UMA.

2.2 PACKET DATA ACCESS

Functions which create and / or access a network data connection using HTTP or HTTPS.

2.3 SOCKET LEVEL PACKET DATA ACCESS

Functions which create and / or access a network data connection using unicast TCP or UDP sockets, or protocols (other than HTTP and HTTPS) implemented above unicast TCP and UDP. This excludes broadcast IP protocols and any functions which may change settings, addresses, routing, encryption, authentication, or identification information of the IP or lower layer network stacks.

2.4 MESSAGING (SPECIFICALLY SMS AND MMS)

Any function which invokes the sending or Interception of Messages over the air like SMS and MMS. If the underlying execution environment can identify other messaging services such as instant messaging or email, then these may be included in this category.

2.5 SMS – CELL BROADCAST

Any function which invokes the reception by an Application of the data broadcast from the network using the SMS-CB bearer.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

2.6 APPLICATION AUTO-INVOCATION

Auto-invocation implies the ability for an Application to force itself to be executed upon particular trigger events such as boot time, reception of a message or at a particular time.

2.7 LOCAL CONNECTIVITY

Functions accessing streams with local connection capability such as Bluetooth, Infrared, WLAN or serial line. Physical as well as wireless connectivity is included in this functional group (e.g. IEEE 1394, USB etc.). This includes all modes or profiles including, but not limited to modem, file transfer and audio.

2.8 MULTIMEDIA RECORDING

Functions for multimedia recording including real time environmental video, still image and audio information. This comprises mainly the access to the camera and microphone.

2.9 RESTRICTED UICC-ME COMMANDS

Restricted UICC-ME commands are defined as any command that can be sent to the SIM/UICC with the exception of the following commands (which are considered non-restricted):

- SELECT
- READ BINARY
- UPDATE BINARY
- READ RECORD
- UPDATE RECORD
- STATUS

The non-restricted UICC-ME commands will be available for all Applications depending on the capability requested (read/write operation).

The remainder of the commands (those considered as restricted) will only be available for Applications installed in the Manufacturer Approved or Operator Approved Trust Levels. The aim of restricting access to these commands is to prevent the possibility of denial of service attacks on the user (through invalidating the SIM/UICC) or attempting to identify card secrets through multiple use of the GSM algorithm.

2.10 NON NETWORK BASED LOCATION

Functions on the Terminal which allow an Application to determine the current location of the Terminal (e.g. GPS, the European Galileo Positioning System). Assisted GPS is included in this functional group.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

This excludes any functions providing explicitly network-derived information such as the network assistance data used in assisted GPS requests.

Applications connecting to an externally connected local GPS device by calling a serial protocol API are not included by this functional group.

2.11 NETWORK BASED LOCATION FUNCTIONS

Functions on the Terminal which allow an Application to determine the current location of the Terminal. It covers access to information obtained by the Terminal from the network broadcast on control channels which are used to provide information about the location of the user. This could be based upon Cell ID, NMR, BCCH list or other information.

2.12 DRM – ACCESS TO UNENCRYPTED DRM PROTECTED DATA

These functions are those that allow an Application access to the underlying DRM capabilities of the Terminal. Access to Terminal keys and certificates are not included in this definition and shall not be made available to third party Applications which execute under this framework. It covers functions on the Terminal which grant access to unencrypted data flows on the Terminal in the case that this data is normally stored in an encrypted form.

2.13 PROCESS MANAGEMENT

These functions are those which allow access to process management functions on the Terminal, to terminate processes separate from the Application, or to power down the Terminal altogether.

2.14 ACCESS TO AT COMMANDS

Functions which allow any Application on the Terminal to use the AT Interpreter to access other APIs on the Terminal.

2.15 USER INPUT EVENTS

Functions that generate user interface events or read user interface events (e.g. keystrokes) for another Application. Whenever an Application is in the foreground (i.e. has focus), this Application will be the rightful receiver of user input events. Applications running in the background will have to access this functional group in order to read or generate user interface events.

2.16 ACCESS TO DATA FUNCTIONAL GROUPS

The following functional groups relate to the controlled access from applications to data on the terminal.

2.16.1 Read Sensitive SIM/UICC Data

Functions able to read sensitive data stored on SIM/UICC.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

Sensitive SIM/UICC Data is defined as all data which is stored on the SIM/UICC:

- excluding those EFs listed in DF Telecom 3GPP TS 51.011 [3]
- and excluding those EFs which have an equivalent in the SIM/UICC's DF Telecom 3GPP TS 51.011 [3]
- but including the elementary file $\mathrm{EF}_{\mathrm{SMSP}}$

2.16.2 Write Sensitive SIM/UICC Data

Functions able to write sensitive data to the SIM/UICC

2.16.3 Read/Write other SIM/UICC Data

Functions able to read and or write any data other than that defined as sensitive (see 2.16.1) from/ to the SIM/UICC

2.16.4 Write Global Network Configuration Data

Functions writing generic network configuration data which can be used by any Application on the Terminal (including that configuration data on the SIM/UICC). This data is used to define the way in which the Terminal interacts with the network. This includes data such as that defined in the OMA Managed Objects Registry [4] (e.g. Access Point Name (APN) and DNS IP address for GPRS connections, number for SMSC, URI for the MMSC, SSID for WLAN). This does not preclude Approved Applications from making network connections using their own self generated network configuration data. For example, an Approved Application can make a connection to a specific APN, but cannot change the APN which is used as a default by other Applications.

2.16.5 Write Terminal Configuration Data

Functions writing configuration data to the Terminal which is used to define the way in which the Terminal itself operates. This includes UI customisation settings and themes.

2.16.6 File System Control and Access

Functions on the Terminal which enable general access to the Terminal file system. This would include the ability to read other Applications private data. An example of Applications accessing this capability are anti-virus or backup Applications

2.17 OPEN ACCESS FUNCTIONAL GROUPS

The following functional groups have been considered as part of this framework document, but it is considered that access to these groups may be allowed for any level of Application including Unapproved.

2.17.1 Read Global Network Configuration Data

Functions reading generic network configuration data which can be used by any Application on the Terminal. This data is used to define the way in which the Terminal interacts with the network. This includes data such as the Managed Objects as defined in OMA (e.g. Access

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

Point Name (APN) and DNS IP address for GPRS connections, number for SMSC, URI for the MMSC, SSID for WLAN).

2.17.2 Read Terminal Configuration Data

Functions reading configuration data from the Terminal which is used to define the way in which the Terminal itself operates. This includes UI customisation settings and themes.

2.17.3 DRM – Delegation of Playback

These functions are made available to Applications which require the ability to render DRM protected content, but use another Application which has access to the unencrypted DRM protected data on the Terminal to do so. The original Application itself has no access to any unencrypted DRM protected content, or DRM credentials.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

3 TRUST LEVELS

3.1 INTRODUCTION

It is important to categorise add-on Applications, whether pre-loaded or downloaded to Terminals, into different Trust Levels dependent upon their likelihood to have vulnerabilities or Malware contained within them.

Applications whose source cannot be verified cannot be fully trusted by the user of a Terminal. In order to protect the user and the network operator from potential vulnerabilities access by Unapproved Applications to certain key functions of the Terminal are restricted.

Trust Levels assigned to Applications are assumed to be granted by the allocation of a certificate to the Application which is checked by the Terminal against known security credentials to assess whether and to which extent it shall be granted access to certain functions.

3.2 UNAPPROVED

An Unapproved Application is any Application where either there is no certificate or where verification of the certificate fails.

REQ. ID	RECOMMENDATION
ASF-0031	If the Terminal identifies that an Application is signed, but there is no allowed root certificate that validates the signature, then the Terminal SHALL install the Application as Unapproved or disallow installation at the discretion of the Terminal.
ASF-0040	Applications with certificates where the signing authority has a root certificate stored on the SIM/UICC or Terminal, but the root certificate is not mapped to a Trust Level SHALL be assigned by the Terminal to the Unapproved Trust Level.
ASF-0050	Applications which have no certificate SHALL be assigned by the Terminal to the Unapproved Trust Level.

Applications of this type may be very popular. However, as their source may not be verifiable, they leave the user with a higher risk of Malware. Therefore, it is necessary to make certain functions unavailable or restricted to the Application (dependent upon user permission for an action) in order to protect the user from potential abuse.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

REQ. ID	RECOMMENDATION
ASF-0061	Applications whose certificates have expired or not yet become valid MAY be assigned by the Terminal to the Unapproved Trust Level, otherwise installation SHALL NOT be granted.

3.3 APPROVED

An Approved Application is one which is signed by a certificate which has a valid certificate chain to a root certificate which is stored on the Terminal as an “Approved Trust Level” certificate.

Applications of this type have a limited risk of Malware as they have a valid certificate and been signed by an Approved Authority whose root certificate is available on the Terminal.

The signing authority (or a delegate of the signing authority) shall use means to ensure a reasonable level of trust in this signed Application. These should include:

- Thorough developer authentication.
- Legal, contractual bindings with the developer.
- Declarative statements (e.g. that the Application is non-malicious, the set of functional groups required).
- Application testing and validation.
- The ability for an Application to be revoked.
- The developer shall be required to indicate at Application certification which functional groups are required for the Application. If the AEE supports the Principle of Least Privilege model for permission control, only these functional groups shall be made available to the Application during execution.

A more substantive description of the requirements for signing schemes is in “Mobile Application Security Requirements For Mobile Application Signing Schemes” [1].

3.4 ENTERPRISE APPROVED

An Enterprise Approved Application is one which is signed by a certificate which has a valid certificate chain to a root certificate which is stored on the Terminal as an “Enterprise Trust Level” certificate.

REQ. ID	RECOMMENDATION
ASF-0070	The enterprise root certificate SHALL only be provisioned on a Terminal by an operator (in the case that the Terminals are sold to the enterprise as part of an operator’s service) or by the Manufacturer.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

Applications of this type carry a minimal risk of Malware as at least one of the following is ensured:

- Applications have been subjected to a high level of checking, exceeding those of Approved Applications e.g. the checking on the Application byte/ source code.
- A specific trusted relationship between the developer and the enterprise is in place, with the enterprise accepting liability for the Application.

3.5 OPERATOR APPROVED

An Operator Approved Application is one which is signed by a certificate which has a valid certificate chain to a root certificate which is stored on the Terminal or SIM/UICC as an “Operator Approved Trust Level” certificate.

Applications of this type carry a minimal risk of Malware as at least one of the following is ensured:

- Applications have been subjected to a high level of checking, exceeding those of Approved Applications e.g. the checking on the Application byte / source code.
- A specific trusted relationship between the developer and the operator is in place, with the operator accepting liability for the Application.

This scheme should not be used to sign Applications submitted by arbitrary third party developers. It should only be used in the case where the operator has an established commercial relationship with the developer.

3.6 MANUFACTURER APPROVED

A Manufacturer Approved Application is one which is signed by a certificate which has a valid certificate chain to a root certificate which is stored on the Terminal as a “Manufacturer Trust Level” certificate.

Manufacturer Approved refers to Applications signed by the Manufacturer and deployed to the Terminal by the user after the pre-shipment customisation process.

Applications integrated by the Manufacturer and shipped with the Terminal before the Terminal reaches the user are considered part of the operating system and are not affected by this document, having full access to any capability provided by the Terminal.

Applications of this type carry a minimal risk of Malware as at least one of the following is ensured:

- Applications have been subjected to a high level of checking, exceeding those of Approved Applications e.g. the checking on the Application byte/ source code.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

- A specific trusted relationship between the developer and the Manufacturer is in place, with the Manufacturer accepting liability for the Application.

REQ. ID	**RECOMMENDATION**
ASF-0080	A Manufacturer signing scheme SHOULD NOT be used to sign Applications submitted by arbitrary third party developers. It should only be used in the case where the Manufacturer has an established commercial relationship with the developer.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

4 INSTALLATION

This section defines the behaviour of the Terminal from the point of installation of an Application.

REQ. ID	RECOMMENDATION
ASF-0085	Where an Application does not require installation prior to execution, the Terminal SHALL provide a security mechanism which checks prior to the execution the Trust Level it is assigned to, the functional groups it is allowed to access on execution and the corresponding access conditions.
ASF-0091	The Terminal SHALL provide a security mechanism which checks at installation whether an Application may be installed, the Trust Level it is assigned to, the functional groups it is allowed to access on execution and the corresponding access conditions.
ASF-0100	The Application's assignment to one of the predefined Trust Levels SHALL be confirmed by verifying the signature over the Application via its Application Certificate and a corresponding root certificate on either the SIM/UICC or the Terminal.
ASF-0110	The Terminal SHOULD apply the Principle of Least Privilege in allowing Applications to access APIs: that is, if an Application provides, at installation time, a declaration of the normative functional groups (as defined in this document) it needs to access, the Terminal SHALL prevent access to all other functional groups.
ASF-0120	The AEE SHOULD support a mechanism that enables Applications to declare functional groups it wants to use prior to installation.

4.1 *REVOCATION MANAGEMENT*

REQ. ID	RECOMMENDATION
ASF-0131	The device SHALL support a revocation mechanism that allows the device to determine during installation whether an Application has been revoked. This revocation mechanism SHOULD be the Online Certificate Status Protocol – OCSP (RFC2560) [5] but other methods with equivalent functionality MAY be supported instead.
ASF-0141	The use of revocation mechanisms at Application installation is optional, and SHALL be configured during Terminal customisation.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

REQ. ID	RECOMMENDATION
ASF-0150	It MUST be possible to use the revocation checking mechanism for Applications corresponding to any recognised Trust Level other than Unapproved.
ASF-0161	The Terminal SHOULD support a mechanism to also prevent Blacklisted Unapproved Applications from installation.
ASF-0170	If the Terminal is configured to perform a revocation check, the Terminal SHALL do this prior to the installation of an Application.
ASF-0180	Where an Application is found by the Terminal to be revoked, the Terminal SHALL NOT allow installation of the Application
ASF-0191	If the device supports ASF-0170 (i.e the Terminal is configured to perform a revocation check), but where the Terminal is unable to confirm revocation status for an Application (e.g. the user is out of coverage or the revocation status cannot be obtained), the device SHALL support a configuration option to enable either: ▪ installation of the Application without any additional user prompting ▪ installation of the Application only with an additional user prompting ▪ installation of the Application is disallowed The default value SHALL be installation without a prompt.
ASF-0201	If the Terminal supports and is configured to perform a revocation check and where the revocation status is unclear (e.g. the user is out of coverage or the revocation status cannot be obtained), and unless installation has been denied (see ASF-0191, the Application SHALL be assigned to the Ttrust Level corresponding to the Application’s certificate with access permissions granted as defined for that Trust Level.

NOTE. There are legal issues which have to be carefully considered regarding revocation of an Application. These include decisions on when to consider an Application as malicious and hence the need to revoke, whether or not to revoke on behalf of the user, the responsible parties for any associated costs etc.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

4.2 INSTALLATION OF UNAPPROVED APPLICATIONS

REQ. ID	RECOMMENDATION
ASF-0211	If an Unapproved Application declares that any of the circuit switched connections, socket level packet data access, packet data access, messaging, multimedia recording or local connectivity functions will be used, or the Terminal is unable to establish whether the Application will use them, the Terminal SHALL deliver a notification, informing the user that the Application’s developer cannot be verified and therefore that the Application is from an unknown source and could be malicious.
ASF-0221	If an Unapproved Application declares that any of the following functions; circuit switched connections, socket level packet data access, packet data Access, messaging, multimedia recording & local connectivity will be used, or the Terminal is unable to establish whether the Application will use them, then installation of the Application MAY be granted upon user permission.
ASF-0241	If an Unapproved Application declares that all of the circuit switched connections, socket level packet data access, packet data access, messaging, multimedia recording, & local connectivity functions will not be used and, therefore, by means of the Principle of Least Privilege, these functions are restricted for that Application, then the Terminal MAY present a notification to the user that the Application is from an untrusted source.

4.3 INSTALLATION OF APPROVED APPLICATIONS

REQ. ID	RECOMMENDATION
ASF-0250	Where an Application is Approved (see section 3.3), the user MAY receive an installation time notification with information on the developers identity, the signing status of an Application and functions used.
ASF-0271	Where an Application is Approved (i.e. signed by a certificate which has a valid certificate chain to a root certificate which is stored on the Terminal as an “Approved Trust Level” certificate, see section 3.3), the Application SHALL be assigned to the “Approved” Trust Level.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

REQ. ID	RECOMMENDATION
ASF-0280	If an Approved Application is able to force itself to be invoked automatically, rather than by user request (Application Auto Invocation – Section 2.6), the user SHOULD be given a prompt explaining that this might happen (along with the list of other functional groups of relevance used by the Application) and giving the opportunity to abort installation.

4.4 INSTALLATION OF OPERATOR, ENTERPRISE OR MANUFACTURER APPROVED APPLICATIONS

REQ. ID	RECOMMENDATION
ASF-0291	Where an Application is signed by a certificate which has a valid certificate chain to a root certificate which is stored on the Terminal or SIM/UICC as an Operator Approved Trust Level certificate (see section 3.5) the Application SHALL be assigned to the Operator Approved Trust Level.
ASF-0301	Where an Application is signed by a certificate which has a valid certificate chain to a root certificate which is stored on the Terminal as an Enterprise Approved Trust Level certificate (see section 3.4), the Application SHALL be assigned to the Enterprise Approved Trust Level.
ASF-0311	Where an Application is signed by a certificate which has a valid certificate chain to a root certificate which is stored on the Terminal as a Manufacturer Approved Trust Level certificate (see section 3.6), the Application SHALL be assigned to the Manufacturer Approved Trust Level.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

5 ARCHITECTURAL MAPPING

The table below shows the functional groups which are restricted from Applications depending on which Trust Level they have been assigned to.

An “x” placed in the table indicates that a particular functional group shall not be available to Applications of the given Trust Level (e.g. an Unapproved Application shall not have access to write Terminal configuration data under any circumstances). If an “x” is not present, the functional group may be granted to an Application under the prompting regime described in Section 6 “Run Time Prompting” and according to the Principle of Least Privilege.

REQ. ID	RECOMMENDATION
ASF-0320	A Terminal SHALL support trust policy matrices stored on the Terminal.
ASF-0330	A Terminal SHALL support the association of Terminal-based trust policy matrices with distinct execution environments.

Trust Level **FUNCTIONAL GROUPS**	Circuit Switched Connections	Socket Level Packet Data Access	Packet Data Access	Messaging	SMS-Cell Broadcast	Application Auto Invocation	Local Connectivity	Multimedia Recording	Read/Write other SIM/UICC Data	Read Sensitive SIM/UICC Data	Write Sensitive SIM/UICC Data	Restricted UICC-ME Commands	Write Global Network Configuration Data	Write Terminal Configuration Data	Non-Network Based Location	Network Based Location Iinformation	DRM – Access To Unencrypted DRM Protected data	Process Management	Access to AT Commmands	User Input Events	File System Control and Access
Unapproved					x	x			x	x	x	x	x	x	x	x	x	x	x	x	x
Approved										x	x	x	x			x	x	x	x		x
Enterprise Approved										x	x	x	x			x	x		x		x
Operator Approved																	x				
Manufacturer Approved																					

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

5.1 PERMISSIONS FOR UNAPPROVED APPLICATIONS

REQ. ID	RECOMMENDATION
ASF-0360	An Application assigned to the Unapproved Trust Level SHALL NOT be granted access to the 'SMS-Cell Broadcast' functional group defined in section 2.
ASF-0370	An Application assigned to the Unapproved Trust Level SHALL NOT be granted access to the 'Application Auto Invocation' functional group defined in section 2.
ASF-0385	An Application assigned to the Unapproved Trust Level SHALL NOT be granted access to the 'Read/Write other SIM/UICC Data' functional group defined in section 2.
ASF-0390	An Application assigned to the Unapproved Trust Level SHALL NOT be granted access to the 'Read Sensitive SIM/UICC Data' functional group defined in section 2.
ASF-0400	An Application assigned to the Unapproved Trust Level SHALL NOT be granted access to the 'Write Sensitive SIM/UICC data' functional group defined in section 2.
ASF-0410	An Application assigned to the Unapproved Trust Level SHALL NOT be granted access to the 'Restricted UICC-ME Commands' functional group defined in section 2.
ASF-0420	An Application assigned to the Unapproved Trust Level SHALL NOT be granted access to the 'Write Global Network Configuration Data' functional group defined in section 2.
ASF-0430	An Application assigned to the Unapproved Trust Level SHALL NOT be granted access to the 'Write Terminal configuration data' functional group defined in section 2.
ASF-0441	An Application assigned to the Unapproved Trust Level SHALL NOT be granted access to the 'Non-Network based location' functional group defined in section 2.
ASF-0450	An Application assigned to the Unapproved Trust Level SHALL NOT be granted access to the 'Network based location information' functional group defined in section 2.
ASF-0460	An Application assigned to the Unapproved Trust Level SHALL NOT be granted access to the 'DRM – Access to Unencrypted DRM Protected Data' functional group defined in section 2.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

REQ. ID	RECOMMENDATION
ASF-0470	An Application assigned to the Unapproved Trust Level SHALL NOT be granted access to the 'Process Management' functional group defined in section 2.
ASF-0480	An Application assigned to the Unapproved Trust Level SHALL NOT be granted access to the 'Access to AT Commands' functional group defined in section 2.
ASF-0490	An Application assigned to the Unapproved Trust Level SHALL NOT be granted access to the 'User Input Events' functional group defined in section 2.
ASF-0500	An Application assigned to the Unapproved Trust Level SHALL NOT be granted access to the 'File System Control and Access' functional group defined in section 2.

5.2 PERMISSIONS FOR APPROVED APPLICATIONS

REQ. ID	RECOMMENDATION
ASF-0510	An Application assigned to the Approved Trust Level SHALL NOT be granted access to the 'Read Sensitive SIM/UICC Data' functional group defined in section 2.
ASF-0520	An Application assigned to the Approved Trust Level SHALL NOT be granted access to the 'Write Sensitive SIM/UICC data' functional group defined in section 2.
ASF-0530	An Application assigned to the Approved Trust Level SHALL NOT be granted access to the 'Restricted UICC-ME Commands' functional group defined in section 2.
ASF-0540	An Application assigned to the Approved Trust Level SHALL NOT be granted access to the 'Write Global Network Configuration Data' functional group defined in section 2.
ASF-0550	An Application assigned to the Approved Trust Level SHALL NOT be granted access to the 'Network Based Location Information' functional group defined in section 2.
ASF-0560	An Application assigned to the Approved Trust Level SHALL NOT be granted access to the 'DRM – Access to Unencrypted DRM Protected Data' functional group defined in section 2.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

REQ. ID	RECOMMENDATION
ASF-0570	An Application assigned to the Approved Trust Level SHALL NOT be granted access to the 'Process Management' functional group defined in section 2.
ASF-0580	An Application assigned to the Approved Trust Level SHALL NOT be granted access to the 'Access to AT Commands' functional group defined in section 2.
ASF-0590	An Application assigned to the Approved Trust Level SHALL NOT be granted access to the 'File System Control and Access' functional group defined in section 2.

5.3 PERMISSIONS FOR ENTERPRISE APPLICATIONS

REQ. ID	RECOMMENDATION
ASF-0600	An Application assigned to the enterprise Trust Level SHALL NOT be granted access to the 'Read Sensitive SIM/UICC Data' functional group defined in section 2.
ASF-0610	An Application assigned to the enterprise Trust Level SHALL NOT be granted access to the 'Write Sensitive SIM/UICC data' functional group defined in section 2.
ASF-0620	An Application assigned to the enterprise Trust Level SHALL NOT be granted access to the 'Restricted UICC-ME Commands' functional group defined in section 2.
ASF-0630	An Application assigned to the enterprise Trust Level SHALL NOT be granted access to the 'Write Global Network Configuration Data' functional group defined in section 2.
ASF-0640	An Application assigned to the enterprise Trust Level SHALL NOT be granted access to the 'Network Based Location Information' functional group defined in section 2.
ASF-0650	An Application assigned to the enterprise Trust Level SHALL NOT be granted access to the 'DRM – Access to Unencrypted DRM Protected Data' functional group defined in section 2.
ASF-0660	An Application assigned to the enterprise Trust Level SHALL NOT be granted access to the 'Access to AT Commands' functional group defined in section 2.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

REQ. ID	RECOMMENDATION
ASF-0670	An Application assigned to the enterprise Trust Level SHALL NOT be granted access to the 'File System Control and Access' functional group defined in section 2.

5.4 *PERMISSIONS FOR OPERATOR AND MANUFACTURER APPLICATIONS*

REQ. ID	RECOMMENDATION
ASF-0680	An Application assigned to the Operator Approved Trust Level SHALL NOT be granted access to the 'DRM – Access to Unencrypted DRM Protected Data' functional group defined in section 2.

REQ. ID	RECOMMENDATION
ASF-0691	The Terminal SHALL allow Applications assigned to the Manufacturer Approved Trust Level to be granted access to all functional groups defined in section 2.
ASF-0702	If a Manufacturer or operator Application declares that it will use Network Based Location capabilities, the AEE SHOULD inform the user during installation time about this fact so the user knows that the Application can access his/her location data at any time during the Application life cycle.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

6 RUN TIME PROMPTING

6.1 PROMPTING FOR UNAPPROVED APPLICATIONS

Most sensitive functions are not able to be accessed by Unapproved Applications. The only exceptions to this are for access to Circuit switched connections, Socket level packet data access, Packet Data Access, Messaging, Local connectivity and Multimedia Recording. For each of these functional groups, this section defines the run-time prompts that shall be implemented by the AEE, the mandatory choices and the actions required by the user to allow or reject an Application from using that functional group.

6.1.1 Permission Types

REQ. ID	*RECOMME*NDATION
ASF-0705	Allowed - No user interaction is required. The access to a function in a Functional Group SHALL always be granted. An Unapproved Application can use the respective function without restrictions.
ASF-0710	One shot – A one shot prompt is that which requires a user to be notified if a particular functional group is requested by an Unapproved Application. The user SHALL be given a choice to allow or disallow the access of that Application to the functional group requested. Every single request for access to APIs from the functional group SHALL require a new prompt for the user. The AEE SHALL prevent access to APIs in the requested functional group until such time as the user allows the access.
ASF-0720	Session – A session prompt is that which requires the user to be notified if a particular functional group is requested by an Unapproved Application. The user SHALL be given the choice to allow or disallow the access of that Application to the functional group requested. The acceptance by the user of a session prompt SHALL allow an Unapproved Application to make use of the functional group requested as long as the following continue to apply: • The Application is still running on the Terminal • The Terminal has not been switched off or placed in standby mode The AEE SHALL prevent access to APIs in the requested functional group until such time as the user allows the access.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

REQ. ID	*RECOMMEN*DATION
ASF-0730	Blanket – A blanket prompt is that which requires a user to be notified if a particular functional group is requested by an Unapproved Application. The user SHALL be given a choice to allow or disallow the access of that Application to the functional group requested. The acceptance by the user of this prompt SHALL allow an Unapproved Application to make use of the functional group requested at any time thereafter without any further prompting. The AEE SHALL prevent access to APIs in the requested functional group until such time as the user allows the access.

6.1.2 Packet Data Access

REQ. ID	*RECOMMEND*ATION
ASF-0741	For Unapproved Applications, the Terminal SHALL present the user with a run time prompt every time a new data session is initiated by the Application. This includes if a network data session was closed for any reason (e.g. either the Application or network closed the session) and the same Application requires a subsequent “packet data access” session. If the packet data access causes a user prompt for permission to create a circuit-switched data connection, this prompt MAY be omitted.
ASF-0741.1	The prompt SHALL warn the user that a data connection is being established and identify the Unapproved Application that is making the connection to the packet data access functions.
ASF-0741.2	The prompt SHALL provide the capability to disallow once or disallow always or to allow this connection. The default option SHOULD be to disallow the connection to the packet data access functions.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

6.1.3 Socket Level Packet Data Access

REQ. ID	RECOMMENDATION
ASF-0745	For Unapproved Applications, the Terminal SHALL present the user with a run time prompt every time a new data session is initiated by the Application. This includes if a network data session was closed for any reason (e.g. either the Application or network closed the session) and the same Application requires a subsequent "socket level packet data access" session. If the socket level packet data access causes a user prompt for permission to create a circuit-switched data connection, this prompt MAY be omitted.
ASF-0745.1	The prompt SHALL warn the user that a data connection is being established and identify the Unapproved Application that is making the connection to the socket level packet data access functions.
ASF-0745.2	The prompt SHALL provide the capability to disallow once or disallow always or to allow this connection. The default option SHOULD be to disallow the access to the socket level packet data access functions.

6.1.4 Prompting for Messaging

REQ. ID	RECOMMENDATION
ASF-0751	If an Unapproved Application attempts to call the messaging function(s) on a Terminal, the AEE SHALL present the user with a one-shot prompt.
ASF-0751.1	Each single message sent SHALL require a separate prompt. If a message will be sent as multiple SMS messages, the prompt SHOULD include the number of SMSs that will be sent.[6]
ASF-0751.2	The prompt SHALL inform the user of the message destination address(es) (e.g. E164 number, name or other applicable address type).
ASF-0751.3	The prompt SHALL warn the user that a message is being sent and identify the Unapproved Application that is sending the message.

[6] In the case of MMS, a message sent to multiple recipients will be considered as a unique message in terms of prompting.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

REQ. ID	*RECOMMENDATION*
ASF-0751.4	The prompt SHALL provide the capability to disallow once or disallow always or to allow the sending of the message. The default option SHOULD be to disallow the message being sent.

6.1.5 Prompting for Local Connectivity

REQ. ID	*RECOMMENDATION*
ASF-0761	If an Unapproved Application attempts to call the local connectivity function(s) on a Terminal, the AEE SHALL present the user with a session based prompt. A connection to any separate local connectivity type (e.g. Bluetooth, WiFi and InfraRed) SHALL each be considered as requiring a separate session and, therefore, a separate session based prompt SHALL be required for each.
ASF-0761.1	The prompt SHALL warn the user that a local connection is being requested and identify the Unapproved Application that is making the connection.
ASF-0761.2	The prompt SHALL provide the capability to disallow once or disallow always or to allow this connection. The default option SHOULD be to disallow the connection to the local connectivity functions.
ASF-0761.3	In addition to that described in section ASF-0720, a local connectivity session SHALL be considered to have terminated if it was closed for any reason (e.g. the Unapproved Application, remote Terminal or network closed the session).

6.1.6 Prompting for Multimedia Recording

REQ. ID	*RECOMMENDATION*
ASF-0771	If an Unapproved Application attempts to call the microphone recording function(s) on a Terminal, the AEE SHALL present the user with a session based prompt which applies to the use of the microphone only.
ASF-0772	If an Unapproved Application attempts to make use of the camera functions (still or video) on a Terminal, the AEE SHALL present the user with a session based prompt which applies to the use of the camera for still and video images as well as microphone recording.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

REQ. ID	RECOMMENDATION
ASF-0773	If either ASF-0771 or ASF-0772 applies, the prompt SHALL warn the user of the type of multimedia recording being requested and identify the Unapproved Application that is requesting it.
ASF-0774	If either ASF-0771 or ASF-0772 applies, the prompt SHALL provide the capability to disallow once or disallow always or to allow this access to the camera and/or microphone. The default option SHOULD be to disallow the access.

6.1.7 Prompting for Circuit Switched Connections

REQ. ID	RECOMMENDATION
ASF-0785	***If an Una***pproved Application attempts to call the circuit switched connection function(s) on a Terminal, the AEE SHALL present the user with a one-shot based prompt. If the function(s) would also result in the user being prompted to select a network access point, then the two prompts SHOULD be combined.
ASF-0785.1	Each single call SHALL require a separate prompt.
ASF-0785.2	The prompt SHALL inform the user of the call destination (e.g. E164 number, name or other applicable address type).
ASF-0785.3	The prompt SHALL warn the user that a call is being made and identify the Unapproved Application that is making the circuit switched connection.
ASF-0785.4	The prompt SHALL provide the capability to disallow once or disallow always or to allow the call set-up. The default option SHOULD be to disallow once.

6.1.8 Open Access Functional Groups

REQ. ID	RECOMMENDATION
ASF-0787	Where an Unapproved Application attempts to access any of the functional groups defined in section 2.17, access SHOULD be Allowed as defined in section ASF-0705

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

6.2 PROMPTING FOR APPROVED, ENTERPRISE, OPERATOR AND MANUFACTURER APPLICATIONS

REQ. ID	RECOMMENDATION
ASF-0790	Following the successful installation of an Approved Application onto a Terminal, the Terminal MAY provide mechanisms to allow the user to limit or keep track of the sensitive functional groups (as defined in section 2) used by Approved Applications on the Terminal. This could be to monitor the expenditure incurred by an Application. Examples of such mechanisms are: • Prompts before chargeable events such as voice calls, message transmission or network access. (Such prompts could be presented every time the API is called, or every n messages, or every m Mbytes of data transmitted) • Logs kept of chargeable events — which could be viewed by the user
ASF-0800	Run time prompts for Applications MAY be presented in the Approved, enterprise, operator and Manufacturer Trust Levels for non-restricted functional groups (as defined in section 2).
ASF-0810	If prompts are implemented, the prompting regime in the Approved, enterprise, operator and Manufacturer Trust Levels SHALL allow the user to control prompts independently for each Application.

.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

7 TERMINAL REQUIREMENTS

To complement the security framework as defined in sections 4, 5 & 6, the following requirements are defined:

REQ. ID	RECOMMENDATION
ASF-0820	All installed Applications either on the Terminal or any related removable media SHALL fall under the control of this security framework.
ASF-0841	Installation of root certificates used by the ASF SHALL NOT be possible except at manufacture or by using a post-manufacture mechanism involving operator or Manufacturer authentication.
ASF-0860	The Terminal SHALL support root certificates for the operator Trust Level stored on the Terminal.
ASF-0870	The Terminal SHALL be capable of supporting at least two root certificates for each supported Trust Level.
ASF-0880	For each AEE on the Terminal the root certificates for any corresponding “OMTP recommended” Application certification programme(s) SHOULD be pre-loaded onto the Terminal.
ASF-0890	The user or any local Application (Unapproved or Approved) SHALL NOT be able to delete root certificates for the Approved, Enterprise, Operator or Manufacturer Approved Trust Levels, except as given in requirement ASF-0900.
ASF-0900	When a Terminal is reset to factory defaults, the Terminal SHALL re-install all factory preset root certificates and remove all others. Certificates stored on the SIM/UICC will remain unaffected by this procedure.
ASF-0910	When an executable or Application installation file is received as an attachment to any kind of message, or as a Bluetooth, infra red, data cable or other remote file transfer (excluding authenticated Terminal Management), the file SHALL NOT be automatically launched and the user SHALL NOT be prompted to launch the file. It SHALL NOT be launched unless the user takes a deliberate action to do so.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

REQ. ID	RECOMMENDATION
ASF-0920	Installation files on a memory card MAY be auto-launched when the memory card is inserted in the phone. If they are auto launched, the Terminal SHALL present a prompt (including information on the Applications to be installed) allowing the user to choose whether the Applications on the memory card can be installed.
ASF-0930	The AEE SHALL prevent any Application in any Trust Level other than the Operator or Manufacturer Approved Trust Level from accessing the active or previously used RAND, SRES, Kc, AUTN, CK or IK. Applications may be provided with RAND in the context of Generic Bootstrapping Architecture (GBA).
ASF-0940	To facilitate the customisation of the number of Trust Levels and policy matrix per Trust Level, Terminals SHALL support the Trust Levels defined in this requirements document, and an additional two which are available for customisation by the operator.
ASF-0960	The Terminal SHALL support a mechanism to associate Terminal based root certificates with a specific AEE_where the information required to do this is available to the Terminal.
ASF-1050	The aim of this OMTP recommendation is to state the agreed policies for most operators for the number of Trust Levels and the policy matrix per Trust Level. However, for Terminals that operators resell, the operator SHALL have sole authority to specify ex-factory:
ASF-1050.1	• The number and source of installed signing root certificates (public key).
ASF-1050.2	• The policy matrix ('architectural mapping') per Trust Level and AEE (i.e. the operator may wish to deviate from the OMTP matrix).
ASF-1050.3	• The mapping of signing root certificates to Trust Levels.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

REQ. ID	RECOMMENDATION
ASF-1061	The Terminal SHALL prevent Unapproved and Approved Applications from intercepting SMS messages targeted at well known ports (as defined in the WMA 1.1 specification [6]) on the Terminal. (E.g. wap-push 2948 WAP PUSH wap-pushsecure 2949 WAP PUSH SECURE wv-csp-sms-cir 3716 WV CSP SMS CIR Channel wv-csp-sms 3590 WV CSP SMS Binding)
ASF-1071	It SHALL NOT be possible for Unapproved Applications to send a file that is recognised by the AEE as installation or executable file type, as part of a message attachment when invoking a function of the Messaging Functional Group (as described in section 2).
ASF-1080	If WiFi, Bluetooth or infrared are switched off, Unapproved Applications SHALL NOT be able to switch them on without user agreement.
ASF-1090	Applications SHALL be granted some Application Data space for their own specific data. An example of specific Application Data is high scores for games.
ASF-1100	The Application Data area SHOULD be of a restricted size to protect against denial of service attacks by filling the storage of the Terminal.
ASF-1110	The Application Data area SHALL be protected from other Applications unless specifically allowed by that Application or because the other Application has access to the “File system control and access” functional group.
ASF-1120	The device SHALL prevent any Application from registering to intercept any received messages on an SMS Port that has already been registered by another Application.

7.1 INTERACTION WITH THE SIM/UICC

REQ. ID	RECOMMENDATION
ASF-1130	A Terminal SHALL support the mechanism SCPROV [7] to read root Certificates from the SIM/UICC. These root certificates SHALL be used to authorise Operator Approved Trust Level Applications in accordance with requirements ASF-1160, ASF-1170, ASF-1180, ASF-1190 and ASF-1200[7]

[7] Operators shall use the applicable root certificate to sign Applications in the Operator Approved Trust Level for each Application Execution Environment on the Terminal.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

REQ. ID	**RECOMMENDATION**
ASF-1140	If the Terminal detects an operator Trust Level root certificate on the SIM/UICC and is able to determine that the root certificate is relevant to a particular AEE, this root certificate SHALL be used to verify Applications for the applicable execution environment.
ASF-1150	The Terminal SHOULD support a standardised mechanism to associate SIM/UICC based root certificates with specific AEEs.
ASF-1160	To determine the Operator Approved root certificate which the Terminal should use to authorise operator level Applications, the Terminal SHALL first check for a stored certificate on the SIM/UICC. For each supported AEE on the Terminal, if there are any related Operator Approved roots on the SIM/UICC, the Terminal SHALL use these to authorise an Operator Trust Level Application of the same AEE. The device MAY additionally require a second signature to be validated against device-based roots. For each supported AEE on the device, if there are no related Operator Approved roots on the SIM/UICC, the Terminal SHALL use device-based roots to authorise operator level Applications.
ASF-1170	Terminals SHOULD support a mechanism allowing a Terminal based root certificate to be verified as associated with the operator that issued the currently-installed SIM/UICC.
ASF-1180	If the Terminal supports the mechanism in ASF-1170, then any Terminal-based root certificate SHOULD NOT be utilised as an operator root certificate unless it can be verified as associated with the operator that issued the currently-installed SIM/UICC.
ASF-1190	If Requirement ASF-1140 is supported, then Signatures of Applications SHALL be re-verified when a change of SIM/UICC is detected (a change of the SIM/UICC may be detected by comparing the ICCID of the previous SIM/UICC with that of the new SIM/UICC).
ASF-1200	If Requirement ASF-1140.is supported, then when the SIM/UICC is changed, the Terminal SHALL ensure that any Applications whose signature validation fails be disabled or run as Unapproved at the discretion of the Terminal. (see ASF--0031).

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

7.2 DATA PROVIDED BY APPLICATIONS

The data that is stored on a User's Terminal consists of many different types including data stored for temporary purposes during the execution of a particular Application. The data may be private and contain personal information about the User. It might also be photos or documents which have been created but not backed up. This type of data can be considered to be sensitive and therefore should be protected from abuse from malware on the Terminal.

However, some data is not particularly sensitive and it may be highly desirable that it can be shared equally between all of the applications which might execute on the Terminal, including those that are Unapproved. It is difficult, therefore, to specify a single method of protecting all data which is written by particular applications. The requirements below provide the means whereby the data that is written by an application can be protected according to the requirements laid down by the application developer.

REQ. ID	RECOMMENDATION	NOTES (FOR INFORMATION ONLY)
ASF-1250	The AEE SHALL allow an Application to write data to the Terminal in such a way that they can be freely read or overwritten by any other Application.	Such type of data is considered as 'open data', i.e. it can be made available for further use by any other application.
ASF-1260	The AEE SHALL allow an Application to write data to the Terminal in such a way that they can only be read or overwritten by that same Application (or by an Application which has access to the functional group "File System Control and Access").	This is the data which an application can be certain is protected from enterprise, approved and unapproved applications (unless it chooses to share it – see ASF-1270)

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

REQ. ID	**RECOMMENDATION**	**NOTES (FOR INFORMATION ONLY)**
ASF-1270	The AEE SHALL allow an Application (the "Data Owning Application") to write data to the Terminal in such a way that read and write access to the Data by other applications ("Data Accessing Applications") are determined by the Data Owning Application itself, through one or both of the following means: • the Data Owning Application exposes APIs to other Applications, and defines a policy for accessing those APIs. the Data Owning Application selects an access control policy based on the Trust Level of a Data Accessing Application, and the AEE enforces that policy.	Two ways of sharing data: 1. In this case, it is for the developer to determine whether it wishes to share its data with another application. The AEE assists the application by providing information such as the trust level or unique identifier (UID) of the requesting application. 2. In this case, the AEE itself restricts access to data according to the policy set by the owning application
ASF-1280	If the AEE allows Applications to expose APIs to other Applications, then the AEE SHOULD allow the Application exposing the API to establish the Trust Level of the Application calling the API.	
ASF-1290	It SHOULD be possible for operators to prohibit implementation of the requirement ASF-1250.	

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

8 FURTHER WORK

The following list expresses those areas where there is a need for further requirements which could be addressed in future versions of this document:

- Potential backwards compatibility issues with other security frameworks.
- Support for SIM/UICC root certificates which may be assigned to any Trust Level for any AEE.
- Issues of revocation, mechanisms such as Certificate Revocation Lists (CRLs) versus OCSP.
- Incident Handling work item needs to address the risk scenario in which an actually revoked Application is installed due to a temporary blocking of a revocation check, requiring a subsequent revocation check (scheduled, or upon Application use).
- The issue of updating the Terminal OTA to configure it to perform revocation checks.
- Support for trust policy matrices stored on the UICC/SIM and associated with distinct execution environments.
- Defining the information to be provided and the customisation of prompts for particular functional groups.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

9 DEFINITION OF TERMS

The table below contains the definition of terms used in this document.

TERM	DESCRIPTION
APPLICATION	OMTP uses a broad definition of “Application” in this document. The term is used to cover active software components such as executables and libraries as well as more passive components such as content and scripts. The Application may be pre-loaded, downloaded to the mobile Terminal via means such as the mobile network, installed via another Application or transferred via infrared connection, Bluetooth, memory card or cable. Typical examples of mobile Applications include games, media players, word processors, security Applications and content. It does exclude firmware and SIM toolkit Applications. Depending on the Application Execution Environment, Applications may consist of one or more files with additional information such as the environment required to run the Application, debugging information, or other information used by the operating system to prepare the program to be run.
APPLICATION DATA	Data that is stored by one Application but which is not available for reading or modification by other Applications on the Terminal unless they are executing at operator or Manufacturer Trust Level.
APPLICATION EXECUTION ENVIRONMENT (AEE)	The Application Execution Environment is that layer which provides an Application with access to the functional groups and specific APIs within those functional groups. It is the AEE which restricts access to some functions for Applications of specific Trust Levels (as defined in this document) and provides prompts to the user as defined in this document.
APPROVED APPLICATION	An Application which is signed by a certificate which has a valid certificate chain to a root certificate which is stored on the Terminal as an “Approved Trust Level” certificate
APPROVED AUTHORITY	An Approved Authority is that which has the capability to pre-install onto the Terminal a root certificate which allows the OS to verify that an Application has been signed by that same authority and hence is granted access to the appropriate Trust Level.
APPROVED TRUST LEVEL	The Trust Level to which Approved Applications are assigned.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

TERM	DESCRIPTION
BLACKLISTED	A "blacklist" is a list of Applications for which installation and execution on a device should be prevented to protect the user and/or operator against any damage. Applications on this list may include those which have been identified as Malware or have a Security Vulnerability.
ENTERPRISE APPROVED	An Enterprise Approved Application is one which is signed by a certificate which has a valid certificate chain to a root certificate which is stored on the Terminal as an “enterprise Trust Level” certificate
INTERCEPTION OF MESSAGES	The ability for an Application to intercept a message which has been received by the Terminal prior to its delivery to the appropriate messaging inbox of the Terminal or by another Application. Interception of Messages may be done by reference to a specific registered port number.
MALWARE	Any program code, programming instruction or set of instructions intentionally constructed with the ability to damage, interfere with or otherwise adversely affect computer programs, data files or operations, handsets, other Terminals, or the network functionalities, including, without limitation, viruses, worms, Trojan horses, spy ware, and programs deliberately carrying out a useless, disruptive, or destructive function not justified by the legitimate running of an Application, such as without limitation creating billable events (e.g. calls, SMS, network connection), changing settings or gathering, forwarding, manipulating, or destroying information of or about the user without appropriate permission. This definition includes any functionalities that exploits a Security Vulnerability.
MANUFACTURER	The company who holds the warranty for the Terminals being sold in the market.
MANUFACTURER APPROVED	A Manufacturer Approved Application is one that is signed by the Manufacturer and deployed to the Terminal by the user after the pre-shipment customisation process.
OPERATOR APPROVED	An Operator Approved Application is one which is signed by a certificate which has a valid certificate chain to a root certificate which is stored on the Terminal or SIM/UICC as an “Operator Approved Trust Level” certificate
PRINCIPLE OF LEAST PRIVILEGE	The idea of the principle is to grant just the minimum possible privileges to permit a legitimate action, in order to enhance protection of data and functionality from faults (fault tolerance) and malicious behaviour (computer security) [8]

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

TERM	DESCRIPTION
SECURITY VULNERABILITY	A flaw in the design or implementation of the Application which can be exploited by malicious entities to use the Application's privileges in unintended ways to damage, interfere with or otherwise adversely affect computer programs, data files or operations, handsets, other Terminals, or network functionality.
SMS PORT	The port on the Terminal to which SMS messages may be targeted. This port number is specified in the SMS User Data Header and indicates to the Terminal for which Application the SMS is targeted.
TERMINAL	Used as an alternative term for a cellular telephone or handset.
TRUST LEVEL	Tiers, domains or levels of assurance which correspond to the level of trust which OMTP place in that Application via an appropriate signing scheme.
UNAPPROVED APPLICATION	Any Application where either there is no certificate or where verification of the certificate fails.
UNAPPROVED TRUST LEVEL	The Trust Level to which Unapproved Applications are assigned.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

10 ABBREVIATIONS

ABBREVIATION	DESCRIPTION
AEE	Application Execution Environment
API	Application Programming Interface
APN	Access Point Name
ASF	Application Security Framework
AT	Attention – from the Hayes AT Command Set, for serial communication
AUTN	Authentication Token – used in UMTS for network authentication
BCCH	Broadcast Control Channel
CK	Cipher Key – used in UMTS
CRL	Certificate Revocation List
DF TELECOM	A SIM/UICC directory containing data such as Abbreviated Dialling Numbers (the SIM/UICC phonebook). Ref: 3GPP TS 51.011 [3]
DNS	Domain Name System
DRM	Digital Rights Management
EF	An Elementary File on the SIM card. Ref:
GBA	Generic Bootstrapping Architecture
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HTTP	Hyper Text Transport Protocol
HTTPS	Secure HTTP
ICCID	Integrated Circuit Card ID
IEEE	Institute of Electrical and Electronics Engineers
IK	Integrity Key – used in UMTS

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

ABBREVIATION	DESCRIPTION
IP	Internet Protocol
JVP	Java Verified Program
KC	Ciphering Key - the session key for the air interface encryption in GSM
ME	Mobile Equipment
MMC	Multimedia Card
MMS	Multimedia Messaging Service
MMSC	Multimedia Messaging Service Centre
MSISDN	Mobile Station Integrated Services Digital Network
NMR	Network Measurement Results
OCSP	Online Certificate Status Protocol
OMA	Open Mobile Alliance
OMTP	Open Mobile Terminal Platform
OS	Operating System
OTA	Over the Air – A secure download to the Terminal or SIM/UICC.
PIM	Personal Information Management
RAND	Random Number
SCPROV	WAP Smart Card Provisioning specification (see Referenced Documents)
SD	Secure Digital (card)
SIM	Subscriber Identity Module. When referring to the SIM, this also includes the use of the USIM
SMS	Short Message Service
SMS-CB	Short Message Service Cell Broadcast
SMSC	Short Message Centre
SRES	Signed Response – used for the air interface encryption in GSM
SSID	Service Set Identifier

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

ABBREVIATION	DESCRIPTION
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UI	User Interface
UID	global Unique Identifier (of an application)
UICC	Universal Integrated Circuit Card
UMA	Unlicensed Mobile Access
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
WAP	Wireless Application Protocol
WLAN	Wireless Local Area Network

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.

11 REFERENCED DOCUMENTS

NO.	DOCUMENT	AUTHOR	DATE
1	Mobile Application Security: Requirements for Mobile Applications Signing Schemes v1.23	OMTP	January 2007
2	RFC 2119 “Key words for use in RFCs to Indicate Requirement Levels”. http://www.ietf.org/rfc/rfc2119.txt	S Bradner	March 1997
3	3GPP TS 51.011 - Specification of the Subscriber Identity Module	3GPP	2005
4	OMNA Device Management (DM) Managed Object (MO) Registry http://www.openmobilealliance.org/tech/omna/omna-dm_mo-registry.htm	OMA	
5	Online Certificate Status Protocol – OCSP (RFC2560).		
6	Java TM Wireless Messaging API (WMA) Specification – Version 1.1 http://java.sun.com/products/wma/	JCP	12 March 2003
7	WAP Smart Card Provisioning (SCPROV) WAP-186-ProvSC-20010710-a	OMA	2001
8	*The protection of information in computer systems,* Proceeding of the IEEE, vol 63 (no. 9), pp 1278-1308	Jerry H. Saltzer & Mike D. Schroeder	September 1975

End of Document.

© 2008 OMTP Limited. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from OMTP Limited.