DATA TRANSFER

VERSION:	2_0
STATUS:	Approved for publication
DATE OF PUBLICATION:	7th March 2008
OWNER:	OMTP Limited

CONTENTS

This document contains information that is confidential and proprietary to OMTP Limited. The information may not be used, disclosed or reproduced without the prior written authorisation of OMTP Limited, and those so authorised may only use this information for the purpose consistent with the authorisation.

The information contained in this document represents the current view held by OMTP Ltd. 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 Members Access Area.

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.

OMTP CONFIDENTIAL

All information exchanged within OMTP is confidential; Information which is or should only be available within the OMTP membership/participants; this is the default for all information which is shared within OMTP; be it committees or project groups; all documents have the OMTP confidentiality disclaimer;

information which is confidential cannot be shared without prior consent of OMTP (i.e. the Board) to publish information;

”Confidential Information” is defined as information, whether written or oral, relating to a party’s technical, operational, administrative or financial arrangement and any other information which is otherwise expressly stated by that party to be confidential;

1 INTRODUCTION

1.1 DOCUMENT PURPOSE

This document defines the minimum recommendations for the supply, preservation, restoration, synchronisation and Transfer of data throughout the lifecycle of a Terminal.

This document will follow a use-case driven approach to requirements elicitation. The key use cases to be supported are listed within section 3

Note: DRM-protected data may be excluded in any of the use cases defined in the document, subject to DRM-constraints.

1.2 INTENDED AUDIENCE

There are two main audiences for these recommendations:

- Other work streams inside OMTP or other standards development organisations that will take these recommendations as input.
- Terminal equipment and technology vendors, who may chose to support data Transfer features.

It is recognised that there are both standard compliant mechanisms of implementing these requirements (specifically OMA SyncML [1]), and multiple proprietary mechanisms of implementing these requirements. These requirements should apply equally to both.

1.3 CONVENTIONS

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 [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:

DT-####, where

- DT is a 2 letter acronym identifying the subject of this OMTP document
- #### is a 4 digit number that identifies the requirement (e.g. 0020) and which is to be unique within the document

2 DATA GROUPING

The following list represents the different types of data within the scope of the first phase of this task:

2.1 USER DATA

As per the OMTP Application Security Framework [3], User Data is that data, which has been created or stored by a User. Examples of this data include:

- Contact information (including phonebook)
- Messages (including SMS, MMS, IM and Emails)
- Calendar information
- Pictures / video clips
- Media clips (e.g. ring tones, wallpaper, songs, videos, etc)
- User-created files (e.g. notes, documents, and other files created by the User)
- URL lists
- Bookmarks
- Predictive text dictionary
- Calls Registry

This data may be stored on either internal or external memory areas including specific User Data areas on a Smart Card (MMC, SD, SIM etc.).

The definition of “User Data” is independent of whether such data has been rightfully created or stored by the User.

Note: For calls registry data, only the file management use case (Section 3.4) applies.

2.2 DEVICE CONFIGURATION DATA

Data that the User may personalise to change the way a Terminal looks or behaves. Examples of this data include:

- Current theme
- Date/Time settings
- Setting of text input behaviour
- Wallpaper, Screensaver
- Accessibility settings
- Speed dial settings
- Fonts
- Menu personalisation
- Softkey personalisation
- Language setting

2.3 GLOBAL NETWORK CONFIGURATION DATA

This data is used to define the way in which the device interacts with:

- The network/bearer, e.g. GSM, UMTS, GPRS, CDMA, Mobile TV, Bluetooth, GPS, etc.
- Application servers, e.g. MMS, SMS, IM, blog, email, WAP or HTTP

2.4 APPLICATION DATA:

- Game/application installation files (e.g. .sis or .jar files) and game/application specific data which can be read, modified or deleted only by the application which created it, such as high scores for a game
- Themes (as defined in OMTP Customisation: Look & Feel [4])

3 USE CASES

This section includes a brief description of the use cases covered in this task.

It is important to note that DRM-protected data may be excluded in **all use cases**, subject to DRM-constraints, as mentioned in section 1.1.

3.1 BACKUP & RESTORE DATA

This section covers several different scenarios that are treated together because of the similarities they share:

- The User wants to Backup data stored in the Terminal as a method to avoid the permanent loss of content (accidental deletion, Terminal break down, etc.) by restoring the information in the original or replacement Terminal.

- The Operator wants to pre-populate Terminals with a rich set of contents (pictures, videos, music, useful contacts, etc.) to stimulate the User to exploit the functionality of the Terminal and increase the acquisition of content. This use case also covers the possibility for an Operator to pre-populate the Terminal with content at PoS, restoring in Terminal Backups made previously, prior to giving the Terminals to customers.

In summary, the scenarios described above cover the following operations:

- **BACKUP**: copying of data to a repository so that these additional copies may be restored
- **RESTORE**: restoration of data to *exactly the same Terminal* that the Backup was made from. Restoration will overwrite existing data on the Terminal. By definition, Backup & Restore are treated together.

- **TRANSFER**: restoration of data *to a Terminal other than the Terminal* from which the Backup was made. Transfer of data will synchronise with the existing data on the Target Terminal.
- **PRE-POPULATION** (at PoS):
  - NEW DATA: Operator populating the Terminal with content packages, local settings for servers, themes, etc.
  - OLD DATA: additionally, the Operator may want also to populate onto the new Terminal the latest Backup available of the User's data.

The Smart Card is not considered as a repository for a Backup operation in this version of the document, but it has been included as a possible further work item in section 7 However, data that resides on the Smart Card can be backed up from the Smart Card and restored back to the Smart Card.

3.2 TERMINAL-TO-TERMINAL DIRECT TRANSFER

This use case describes how a User Transfers data directly between two Terminals via Local Connection. Data being transferred will synchronise with the existing data on the Target Terminal.

3.3 SYNCHRONISATION BETWEEN MULTIPLE DEVICES

This use case covers the scenario when a User wants to synchronise the contacts, calendar information and messages stored in the Terminal with a Computer or with a Remote Server.

3.4 FILE MANAGEMENT

There are situations when a User of a Terminal would like to send or receive discrete sets of User Data. This use case describes this scenario.

As an example, a User may want to Transfer a selection of music files from a Computer to the Terminal.

4 REQUIREMENTS

4.1 GENERAL REQUIREMENTS

REQ. ID	REQUIREMENT
DT-0010	The Terminal MUST support OTA Backup and OTA Restore as defined in the use case in Section 3.
DT-0020	If the data Transfer requirements are satisfied by a User installable application which by implication is running under the OMTP Application Security Framework [3] then this application MUST conform in behaviour to the requirements set out in OMTP Application Security framework [3].
DT-0030	If the Terminal satisfies data transfer requirement functionality as part of the base functionality of the Terminal (and so the data Transfer requirement functionality) may not be running under an application security framework), then the Terminal functionality MUST take best efforts to ensure the confidentiality and integrity of the data is secure against threats which are pertinent to the driving use cases as defined in section 3.
DT-0040	If the Data Transfer Function is taking place OTA (using a network connection) the behaviour of the data Transfer application should conform to the OMTP Recommended Practices for Connected Applications [5].
DT-0050	For the OTA Data Transfer scenario, it MUST be possible to remotely provision settings necessary for the Transfer process to run effectively.

4.2 BACKUP & RESTORE DATA

This section includes the requirements related with the Backup & Restore use case (see section 3.1 for a brief description of the use case)

REQ. ID	REQUIREMENT

REQ. ID	REQUIREMENT
DT-0060	The Terminal MUST have the capability to Backup to (and Restore/Transfer/pre-populate data from) all of the following: • Computer (via Local Connection and OTA) • Remote Server (via OTA) • Removable storage (e.g. memory card) where applicable (via internal interface)
DT-0070	The Terminal MUST provide the User with a functionality to Backup & Restore and Transfer and pre-populate (old and new data) the following data[1]: • User Data[2] • Device Configuration Data
DT-0080	The mechanism by which the User may initiate a Data Transfer Function MUST be easily discoverable within the User interface.
DT-0090	The Terminal SHOULD provide the User with a functionality to Backup & Restore and Transfer the following data[3]: • Global Network Configuration Data • Application Data

[1]The device will attempt to Backup whatever can be backed up and Restore/Transfer/pre-populate whatever can be restored/transferred/pre-populated, within device and DRM constraints.

[2] This use case does not apply to Calls Registry data

[3] The device will attempt to Backup whatever can be backed up and Restore/Transfer whatever can be restored/transferred, within device and DRM constraints.

REQ. ID	REQUIREMENT
DT-0100	The Operator MUST be able to Restore the following data, when pre-populating (old and new data) the Terminal with data at PoS[4]: • Global Network Configuration Data • Application Data
DT-0110	The Terminal MUST enable the User to initiate a Full Backup process (i.e. saving a copy of a complete data set without merging with a previous Backup).
DT-0120	The Terminal MUST enable the User to initiate a Differential Backup process. Rationale: this is an optimisation requirement. This means that Data Transfer Functions, subsequent to the first pairing, can be implemented efficiently both in terms of time and network usage.
DT-0130	The Terminal MUST enable the User to initiate the Restore and Transfer processes.
DT-0140	The Terminal MUST request User confirmation via an option in the Terminal UI before a Restore process starts.
DT-0150	The Terminal MUST enable the User to cancel the Backup process via an option made available in the Terminal UI.
DT-0160	The Terminal MUST enable the User to cancel the Transfer process via an option made available in the Terminal UI and the Terminal SHOULD return the data to the state it was in before the Transfer process started.
DT-0170	The Terminal SHOULD enable the User to cancel the Restore process and, in that case, the Terminal MUST be able to perform a subsequent Restore process.

[4] The device will attempt to pre-populate the device with whatever can be Pre-populated, within device and DRM constraints.

REQ. ID	REQUIREMENT
DT-0180	The Terminal MUST provide the User with the functionality to automate the Backup process. Requirements in section 4.7 (Automation Requirements) MUST also apply.
DT-0190	For Terminal-initiated automatic OTA Backups, if there has been no change in the data between automatic OTA Backups, the Terminal MUST NOT communicate with the network, except for verifying that the most recent Backup is stored in the Remote Server.
DT-0200	The Terminal MUST provide the User with the functionality to select which data groups or items are included into Backups.
DT-0210	The Terminal MUST allow the User to delete the Backup files stored on the local storage card.
DT-0220	The Terminal MUST enable the User to select one of the following actions to perform in case of conflict[5] when Transferring data to a new Terminal: • Overwrite element on new Terminal • Keep both elements • Ignore element being transferred to a new Terminal Note: this does not imply any specific wording in the UI.
DT-0230	The Terminal MUST inform the User when data cannot be successfully restored during a Transfer process and MUST enable the User to select at least one of the following actions to perform in the new Terminal: • Store the transferred data in the new Terminal • Ignore the transferred data and do not store it in the new Terminal Note: this does not imply any specific wording in the UI.

[5] A conflict happens when the same data exists in the backup file and in the new Terminal

REQ. ID	REQUIREMENT
DT-0240	The Terminal MUST allow the User to view a history of the latest Backup/Restore operation completed. The history MUST contain at least the date and time of the Backup/Restore operation.
DT-0250	The Terminal MUST enable the User to select the bearer (e.g. WiFi, GPRS, EDGE, UMTS, etc) or the Local Connection by which the Backup process takes place.
DT-0260	The Terminal MUST enable the User to select the bearer (e.g. WiFi, GPRS, EDGE, UMTS, etc) or the Local Connection by which the Restore and Transfer process takes place.
DT-0270	The Terminal MUST enable the User to select the storage medium (Remote Server, Computer etc.) for the Backup process.
DT-0280	In the case of DT-0270, the Operator MUST be able to define a default selection on the Terminal for the storage media (e.g. removable storage).
DT-0290	In case of “full-memory” when Backup is underway, the Terminal MUST provide a prompt to the User and the Terminal MUST enable the User to cancel the process or manually delete data (from either Terminal or storage as appropriate) and resume the Backup process.
DT-0300	If the Terminal supports a multitasking environment, the Terminal MUST provide the User with the capability to choose that the Backup or Transfer process is performed in the background.
DT-0310	The Terminal SHOULD NOT prevent normal usage of or behaviour of the Terminal while Backup or Transfer processes are underway, where phone capabilities allow.
DT-0320	The Backup or Restore process MUST be able to Recover from events that may impact on the process (e.g. incoming calls, incoming messages connection lost, power lost, etc.)
DT-0330	The Terminal MUST inform the User about the progress of the Backup & Restore or Transfer processes (if they are not running in background mode) and of the success or failure of these processes.

REQ. ID	REQUIREMENT
DT-0340	The Terminal MUST provide the User with the functionality of automatically appending the date to the name of the Backup file if the Backup file is stored locally, i.e. on a removable storage card.
DT-0350	If there are several backed-up data packages present (e.g. different names and timestamps), the Terminal MUST provide the User with the ability to select the one to be Restored.
DT-0360	It MUST be possible to Pre-populate new and old data to a Terminal without a Smart Card at PoS.

4.3 TERMINAL-TO-TERMINAL DIRECT TRANSFER

This section includes the requirements related to the Terminal-to-Terminal Direct Transfer Use Case (see section 3.2)

REQ. ID	REQUIREMENT
DT-0370	The Terminal MUST provide the User with the functionality to Transfer and receive the following data[6] to or from another Terminal directly via a Local Connection: • User Data[7]
DT-0380	The Terminal SHOULD provide the User with the functionality to Transfer and receive the following data[6] to or from another Terminal directly via a Local Connection: • Application Data
DT-0390	The Terminal MUST enable the User to initiate a Transfer whilst referencing (or in the context of) the source data to be transferred (for User data).
DT-0400	The Target Terminal MUST allow the User to accept or reject the Transfer data session via an option made available in the Target Terminal UI.

[6] The device will attempt to transfer/receive whatever can be transferred/received, within device and DRM constraints.

[7] This use case does not apply to Calls Registry in User Data

REQ. ID	REQUIREMENT
DT-0410	The Source Terminal MUST enable the User to cancel the Transfer process via an option made available in the Source Terminal UI.
DT-0420	The Target Terminal MUST enable the User to cancel the Transfer process via an option made available in the Target Terminal UI.
DT-0430	If the User cancels the Transfer process, the Source Terminal MUST return to the previous data state prior to the start of the Transfer process.
DT-0440	The Terminal MUST provide the User with the functionality to specify that the Transfer will only apply to some types of data (e.g. bookmarks and music).
DT-0450	The Terminal MUST provide the User with the functionality to specify that the Transfer will only apply to some items of data (e.g. selected bookmarks).
DT-0460	The Terminal MUST enable the User to select the Local Connection by which the Transfer process takes place.
DT-0470	The Terminal MUST NOT prevent the receipt of incoming calls, messages or push notifications whilst the Transfer process is underway.
DT-0480	The Terminal SHOULD NOT prevent normal usage of and behaviour on the Terminal while a Transfer process is in progress
DT-0490	The Transfer process MUST be able to Recover from events that may impact on it (e.g. incoming calls, incoming messages, connection lost, power lost, etc.)
DT-0500	The Transfer process SHOULD NOT cause data loss at the Target Terminal.

REQ. ID	REQUIREMENT
DT-0510	The Target Terminal MUST enable the User to select one of the following actions to perform in case of conflict when receiving data: • Overwrite existing element on the Target Terminal • Keep both elements • Ignore element from Source Terminal Note, this does not imply any specific wording in the UI.
DT-0520	The Terminal MUST inform the User about the progress of the Transfer processes and its success or failure.
DT-0530	The Terminal MUST provide a mechanism to enable the User to re-attempt the Transfer in event of failure.
DT-0540	When receiving data, the Target Terminal MUST provide the User with a prompt to select the storage destination (e.g. removable storage, Smart Card) for the data and the Target Terminal MUST then store the data at that location.
DT-0550	It SHOULD be possible to Transfer data without requiring a Smart Card to be present in both the Source Terminal and the Target Terminal.
DT-0560	The Target Terminal SHOULD enable the User to define a default storage media (e.g. removable storage) for data being transferred.
DT-0570	When initiating a Transfer, the Target Terminal SHOULD check that there is enough space available on the Terminal before starting the process.
DT-0580	In the case of “full-memory”, the Target Terminal MUST prompt the User with this information and MUST enable the User to cancel the process or manually delete data in the Target Terminal and resume the Transfer process.
DT-0590	The data Transfer process MUST provide a clear mapping between data fields of items to transferred (such as contact data fields) between devices of different types.
DT-0600	Where mappings are ambiguous, the Terminal MUST provide the UI for the User to determine the appropriate mapping

4.4 SYNCHRONISATION BETWEEN MULTIPLE DEVICES

This section include the requirements related to the Synchronisation Use Case (see section 3.3)

REQ. ID	REQUIREMENT
DT-0610	The Terminal MUST provide the User with functionality to synchronise the following data[8]: • Contact information (including phonebook) • Messages • Calendar information
DT-0620	The Terminal MUST enable the User to initiate a synchronisation process from a Terminal.
DT-0630	The Terminal MUST support synchronisation to a Computer via a Local Connection.
DT-0640	The Terminal MUST support OTA synchronisation to a Remote Server.
DT-0650	The Terminal MUST request User confirmation via an option made available in the Terminal UI before a synchronisation starts when: • The synchronisation process has been initiated from a Computer or a Remote Server.
DT-0660	The Terminal MUST enable the User to cancel the synchronisation process via an option made available in the Terminal UI.
DT-0670	The Terminal MUST support the OTA and cable provisioning of the parameters required for data synchronisation (e.g. the server name/IP, Transfer protocol, User, password, etc.).

[8] The device will attempt to synchronise whatever can be synchronised within device and DRM constraints.

REQ. ID	REQUIREMENT
DT-0680	The Terminal MUST provide the User with the functionality to automate the synchronisation process. The requirements in section 4.7 MUST also apply.
DT-0690	The Terminal MUST provide the User with the functionality to specify that the synchronisation will only apply to some classes of data (e.g. contacts or messages).
DT-0700	The Terminal MUST provide the User with the functionality to specify that the synchronisation will only apply to a set of data items (e.g. groups of contacts or last month messages etc.).
DT-0710	The Terminal MUST enable the User to select one of the following actions to perform in case of conflict[9] when synchronising information: • Overwrite element on the Terminal • Keep both elements • Ignore element received by the Terminal Note: this does not imply any specific wording in the Terminal UI.
DT-0720	The Terminal MUST enable the User to select the bearer (e.g. WiFi, GPRS, EDGE, UMTS etc.) or the Local Connection by which the synchronisation process takes place.
DT-0730	The Terminal SHOULD provide the User with the functionality to specify that the synchronisation process is performed in the background.
DT-0740	If the Terminal supports a multitasking environment, the Terminal MUST provide the User with the functionality to specify that the synchronisation process is performed in the background.

[9] A conflict occurs when the same item has been modified on both the server and the client.

REQ. ID	REQUIREMENT
DT-0750	If the synchronisation process is not running in background mode, the Terminal MUST inform the User about the progress of the synchronisation process and its success or failure
DT-0760	The Terminal SHOULD NOT prevent normal usage of or behaviour of the Terminal while synchronisation process is running.
DT-0770	The Terminal MUST provide a mechanism to allow a synchronisation process to Recover from events that may impact on the process (e.g. incoming calls, incoming messages connection lost, power lost, etc.)
DT-0780	The Terminal MUST support Differential synchronisation processes. Rationale: this is an optimisation requirement. This means that Data Transfer Functions, subsequent to the first pairing, can be implemented efficiently both in terms of time and network usage.
DT-0790	The Terminal MUST support Full Synchronisation process.
DT-0800	The Terminal SHOULD use Differential Synchronisation process in preference to Full Synchronisation process, except when e.g. - A data set is synchronised for the first time - The synchronisation client or the server has lost its change log information specified otherwise by the User
DT-0810	The Terminal MUST provide the User with a mechanism to check which items have been updated following a synchronisation operation.

4.5 FILE MANAGEMENT

This section includes requirements related with the “File Management” Use Case (see section 3.4)

REQ. ID	REQUIREMENT

REQ. ID	REQUIREMENT
DT-0820	The Terminal MUST provide the capability to send data to and receive from all the following: • Computer (via Local Connection and OTA) • Remote Server (via OTA) • Removable Storage (e.g. memory card) where applicable (via internal interface)
DT-0830	The Terminal MUST provide the User with the functionality to receive or send the following transferred data[10]: • User Data
DT-0840	The Terminal MUST enable the User to cancel the receiving or sending process. Note: this action may not necessarily be performed from the Terminal.
DT-0850	The Terminal MUST enable the User to select the storage medium (e.g. internal or removable storage) from which the sending process takes place.
DT-0860	When receiving data, the Target Terminal MUST enable the User to select the storage destination (e.g. internal or removable storage) for the data and MUST then store the data at the selected location.
DT-0870	The Terminal MUST enable the User to select the bearer (e.g. WiFi, GPRS, EDGE, UMTS, etc) or the Local Connection by which the sending process takes place.
DT-0880	The Terminal MUST provide the User with a mechanism to specify that the sending process will only apply to some types of data (e.g. bookmarks or music).
DT-0890	The Terminal SHOULD provide the User with a mechanism to specify that the sending will only apply to some pieces of data (e.g. groups of contacts or last month's messages).

[10] The device will attempt to send or receive whatever can be sent or received within device and DRM constraints.

REQ. ID	REQUIREMENT
DT-0900	The Terminal MUST enable the User to select one of the following actions to perform in case of conflict when receiving information: • Overwrite element on Terminal • Keep both elements • Ignore element from Computer, Remote Server or Removable Storage Note: this does not imply any specific wording in the Terminal UI.
DT-0910	If the Terminal supports a multitasking environment, the Terminal MUST provide the User with the capability to choose that the sending or receiving process is run in the background.
DT-0920	The Terminal SHOULD NOT prevent normal usage of or behaviour of the Terminal while sending or receiving files is in progress.
DT-0930	The Terminal MUST provide a mechanism to allow the sending and receiving process to Recover from events that may impact on the Transfer process (e.g. incoming calls or incoming messages, connection lost, power lost, etc.)
DT-0940	The Terminal MUST inform the User about the progress of the process (if the process is not running in background mode) and its success or failure.

4.6 SECURITY REQUIREMENTTHES

This section covers security requirements identified for the different use cases mentioned in previous sections.

REQ. ID	REQUIREMENT
DT-0950	The Terminal MUST provide the User with a mechanism to Backup & Restore/Transfer/Pre-populate data in a secure way to authenticate the User and ensure the integrity and confidentiality of the data.
DT-0960	When using wireless connections, the Terminal MUST use an encrypted connection for the direct Terminal-to-Terminal Transfer, providing enhanced security and data confidentiality.

REQ. ID	REQUIREMENT
DT-0970	When synchronising using wireless connections, the Terminal MUST use an encrypted connection throughout the process, providing enhanced security and data confidentiality.
DT-0980	When using wireless connections, the Terminal MUST use an encrypted connection for the file Transfer process, providing enhanced security and data confidentiality.
DT-0990	The Terminal MUST provide a mechanism to authenticate the User prior to using OTA or Local Connections for the synchronisation or file Transfer processes.

4.7 AUTOMATION REQUIREMENTS

This section covers requirements related to the automation of the Backup and the Synchronisation processes.

REQ. ID	REQUIREMENT
DT-1000	The Terminal MUST provide the User with a mechanism to automate a Backup or a synchronisation process, or both.
DT-1010	The Terminal MUST provide the User with a mechanism to activate/deactivate the automatic Backup or synchronisation process, or both.
DT-1020	The Terminal MUST provide the User with a mechanism to specify the schedule of automatic Backup processes.
DT-1030	The minimum time interval for automatic OTA Backup or synchronisation processes MUST be configurable by the Operator to avoid network overloads.
DT-1040	If the storage destination or the selected connection is not available when an automatic Backup or synchronisation process is triggered, the Terminal MUST try to restart he automatic process up to a maximum number of attempts.
DT-1050	In the case of DT-1040, the Operator MUST be able to configure the maximum number of attempts.
DT-1060	In the case of DT-1050, if the maximum number of attempts is reached the Terminal MUST be able to retry the automatic synchronisation or Backup process (as described in DT-1040) at a future occasion. If the process fails again, then the Terminal MUST NOT retry the process until a new automatic synchronisation or Backup process is triggered.

REQ. ID	REQUIREMENT
DT-1070	The Terminal MUST provide the User with a mechanism to specify that an automatic process is run in the background.

5 FURTHER WORK

This section gives an indication of those areas that may be addressed in future versions of the document but that cannot be included at the current stage due to lack of standardisation, unavailability, etc.

- The Smart Card as a repository for Backup, Restore and Transfer operations: the final agreement reached by ETSI and 3GPP in favour of USB as the High Speed Interface between the Smart Card and the Terminal makes it possible to incorporate requirements in this area in future versions of the document.

- This document must be actively maintained to keep it consistent with the OMTP Application Security Framework [3], and possible future work in this area pertaining specifically to User Data

6 DEFINITION OF TERMS

TERM	DESCRIPTION
APPLICATION DATA	Data created or stored by an application which can be read, modified or deleted only by the application which created it.
BACKUP	Copying of data to a repository so that these additional copies may be restored (e.g. after a data loss event.)
COMPUTER	User's device such as a PC or laptop. The device may fulfil the following roles: • as a means of facilitating Backup & Restore for a Terminal • as a means of upgrading a User to a new Terminal (Transfer use case) • as the primary device for rendering or editing some content or both, where such content then needs to be synchronised with the Terminal.
DATA TRANSFER FUNCTION	An term that encompasses Backup, Restore, Transfer and Pre-population.
DEVICE CONFIGURATION DATA	Data that the User may personalise to change the way a Terminal looks or behaves.
DIFFERENTIAL OR DIFFERENTIALLY	Data from the Terminal and the other elements are compared to data from the previous state in the Backup/Restore and synchronisation process. Only modified elements are involved in the process e.g. new, deleted, etc.
FULL BACKUP	A Backup of all (selected) files, without merging with a previous Backup.
FULL SYNCHRONISATION	A form of synchronisation process in which all items are compared with each other on a field-by-field basis. In practice, the client sends a complete data set from a database to the server and the server performs a field-by-field synchronisation analysis with the uploaded data and the data in the server.
GLOBAL NETWORK CONFIGURATION DATA	Data used to define the way in which the device interacts with the network/bearer and application servers.
LOCAL CONNECTION	Short-range connection for example Bluetooth, Infrared, home or office LAN, cable, or other User-controlled connection.

TERM	DESCRIPTION
OPERATOR	A business entity that provides communications services to customers in the form of products that include combination of Terminals and Smart Cards.
OVER THE AIR	Over The Air (OTA) implies a wireless connection via a 2G or 3G or other Operator-controlled mobile network.
PRE-POPULATION	Data that the Operator puts onto a Terminal at PoS.
RECOVER	Applies to processes that may be interrupted due to events. A Recover occurs when those events finish and the actions to be performed by the process must be finalised, resulting in the same result as if those events had not happened.
REMOTE SERVER	Server managed by services provider (Operator, manufacturer, third parties etc.) that could be configured in the Terminal to connect via OTA to provide services to the User (e.g. Backup, storage and management).
RESTORE	The exact restoration of data to the same device that the Backup was made from.
SMART CARD	Tamper-resistant device (including trusted-by-the-Operator memory and a trusted-by-the-Operator execution environment) that can communicate with the UE through its interface. The Operators issue Smart Cards in the form of Security or User Identification modules. Possible types of Smart Cards are: SIM (GSM), R-UIM (CDMA); or an application as the USIM (UMTS) or the CSIM (CDMA SIM).
SOURCE TERMINAL	Terminal that initiates a data Transfer.
TARGET TERMINAL	Terminal that receives the transferred data.
TERMINAL	Used as an alternative term for a cellular telephone or handset.
TRANSFER	Copying or moving of data between a Terminal and another Terminal or Remote Server, Computer or Removable Storage.
USER	Refers to the person that operates the Terminal such as the customer, shop assistant at PoS, etc.
USER DATA	Data which has been created or stored by a User on the Terminal.

7 ABBREVIATIONS

ABBREVIATION	DESCRIPTION
3GPP	3rd Generation Partnership Project
CDMA	Code Division Multiple Access
CSIM	CDMA2000 Subscriber Identification Module
DRM	Digital Rights Management
EDGE	Enhanced Data Rates for GSM Evolution
ETSI	European Telecommunications Standards Institute
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communication
HTTP	Hyper Text Transfer Protocol
IM	Instant Messaging
LAN	Local Area Network
MMC	Multimedia Card
MMS	Multimedia Message Service
OMTP	Open Mobile Terminal Platform
OTA	Over The Air
PoS	Point of Sale
R-UIM	Removable User Identity Module
SD	Secure Digital
SIM	Subscriber Identity Module
SMS	Short Message Service
UE	User Equipment

ABBREVIATION	DESCRIPTION
UI	User Interface
UMTS	Universal Mobile Telecommunications System
URL	Universal Resource Locator
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module or User Services Identity Module
WAP	Wireless Application Protocol

8 REFERENCED DOCUMENTS

NO.	DOCUMENT	AUTHOR	DATE
1	OMA SyncML Common Specification V1.2.1	OMA	August 2007
2	RFC2119 “Key Words for use in RFCs to indicate Requirement Levels” http://www.ietf.org/rfc/rfc2119.txt	S Bradner	March 1997
3	OMTP Application Security Framework v2.1 http://www.omtp.org/publications.html	OMTP	September 2007
4	OMTP Customisation: Look & Feel, menu and application integration, v2.0, Release 2 (http://www.omtp.org/publications.html)	OMTP	December 2005
5	OMTP Recommended Practices for Connected Applications v1.5 http://www.omtp.org/publications.html	OMTP	October 2007

-------- END OF DOCUMENT --------