

ETSI TS 170 016 V3.1.1 (2009-02)

Technical Specification

Project MESA; Technical Specification Group - System; Functional Requirements Definition

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/9ab4a8bd-ce36-4046-b824-e06e3510303d/etsi-ts-170-016-v3.1.1-2009-02>

Project
MESA



Reference

DTS/MESA-SYS0070016v311

Keywords

application, interoperability, network,
performance, security, service, TMN

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2009.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™**, **TIPHON™**, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

LTE™ is a Trade Mark of ETSI currently being registered

for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	4
Foreword.....	4
Introduction	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references.....	5
3 Definitions and abbreviations.....	5
3.1 Definitions.....	5
3.2 Abbreviations for Requirement Identification.....	7
4 Functional Requirements.....	7
4.1 Core Functional Requirements	8
4.2 Other Requirements.....	20
History	21

iTeh STANDARD PREVIEW
 (standards.iteh.ai)
 Full standard:
<https://standards.iteh.ai/catalog/standards/sist/9ab4a8bd-ce36-4046-b824-e06e3510303d/etsi-ts-170-016-v3.1.1-2009-02>

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://webapp.etsi.org/IPR/home.asp>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by Public Safety Partnership Project (MESA).

The contents of the present document are subject to continuing work within the Specification Group (SG) and may change following formal SG approval. Should the SG modify the contents of the present document, it will be re-released by the SG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
 - 1 presented to SG for information;
 - 2 presented to SG for approval;
 - 3 or greater indicates SG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The functional requirements in the present document were captured through a series of collaborative workshops over several months that involved members of the Public Safety community as represented by the MESA Service Specifications Group (SSG), and infrastructure vendors and operators in the wireless industry as represented by the MESA Technical Specifications group. Using the Statement of Requirements (TS 170 001 [1]) developed by the MESA SSG and using the MESA Network Architecture (MESA 70.015 [i.1]) as a guide, the MESA group derived the functional requirements found in the present document.

1 Scope

The present document give guidelines for the functional requirements required for a MESA system that is consistent with the Service Specification Group's Statement of Requirements (TS 170 001 [1]) and the Technical Specification Groups Network Architecture (MESA 70.015 [i.1]). The present document is intended to be the input into a gap analysis of existing standards and technologies with an ultimate goal to update the existing standards and technologies to be fully compliant with the functional requirements in the present document.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
 - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
 - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at <http://docbox.etsi.org/Reference>.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

- [1] ETSI TS 170 001: "Project MESA; Service Specification Group - Services and Applications; Statement of Requirements", MESA TS 70.001.

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- [i.1] MESA 70.015: " Project MESA; Technical Specification Group - System; System and Network Architecture ".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

airlink resources: available throughput (voice and data) for a given location that can be shared across all users

authorized principal: principal with permissions to perform specific action(s) or receive specific information (Source OMA Dictionary)

bandwidth: amount of spectrum required for the system

NOTE: See also Channel Bandwidth, Radio Bandwidth.

channel bandwidth: amount of spectrum required for a single channel of the system

components: individual parts that together make up the entire system, generally inclusive of devices

NOTE: See also Nodes, Network Elements.

cooperative use: system able to operate overlapped with another system with the components of each system cooperating, not interfering

dynamic bandwidth: allows bandwidth to be changed to allow more capacity for priority users

effective user data rate: effective throughput (voice and data) as perceived by an end user

forward compatibility: ability for a system to operate with future protocols of itself

logical networks: AWN, EAN, JAN, IAN, and PAN as described in the MESA System and Network Architecture Document

MESA system: complete set of integrated components that provide full communication functionality meeting the MESA Statement of Requirements

network elements: individual parts, that together, make up the entire system, excluding devices or clients

NOTE: See also Components, Nodes.

network functions: user transparent functions of the system, such as authentication proxying for single sign on, mobility support, policy enforcement, etc.

nodes: individual parts that together make up the entire system inclusive of devices and clients

NOTE: See also, Components, Network Elements.

Off-Net: "Off Network", meaning the user does not have access to fixed network services, and access to services is restricted to those that reside in the device or functioning wireless transmitters (vehicle or wireless site)

On-Net: "On Network", meaning the user has access to the fixed network services that reside in data or switching centers

peer-to-peer: service within a device that communicates directly with other devices, and does not communicate with any network component

NOTE: Note that this does not preclude the communication from being carried by the network, only that application level messaging is originated and terminated by services resident on the device.

principal: an entity that has an identity, that is capable of providing consent and other data, and to which authenticated actions are done on its behalf

EXAMPLE: Examples of principals include an individual user, a group of individuals, a corporation, service enablers/applications, system entities and other legal entities. (Source OMA Dictionary).

radio bandwidth: amount of spectrum required for the system (inclusive of all channels used)

run-time: commands are executed as they are given

single sign on: ability for the user to provide authentication credentials once to the system, and the system proxies those credentials to any application or services requiring credentials

system: unless otherwise specified, system refers to the MESA system

untrusted connections: connections where the connecting parties have not conducted prior mutual authentication and authorization

3.2 Abbreviations for Requirement Identification

Requirement format is of the form: xx-xxx-xxx (where x are letters, and n are numbers). The format structure consists of a requirement classification, which is a two letter prefix identifying how the requirement will be documented; followed by three letters identifying functional categorizations of the requirements; followed by a three digit number that allows each requirement to be uniquely identified.

For the purposes of identifying requirements, the following requirement abbreviations apply:

Requirement Classification (first two letter identifiers):

DR	Documentation Requirement
DC	Design Consideration Requirement
IR	Implementation Requirement (Requirement is incumbent upon the entities implementing the technology)
FR	Functional Requirement
LMR	Land Mobile Radio

Requirement Functional Categorization (middle three letter identifiers):

ASC (xx-ASC-xxx)	Requirement originating from the team looking at Applications and Services implications and interactions
AWN (xx-AWN-xxx)	Requirements originating from the team looking at Ancillary Wireless Network implications and interactions
EUD (xx-EUD-xxx)	Requirements originating from the team looking at End User Device implications and interactions. Implementation Requirement (Requirement is incumbent upon the entities implementing the technology)
IOP (xx-IOP-xxx)	Requirements originating from the team looking at interoperability implications and interactions
JRA (xx-JRA-xxx)	Requirements generated from the first round of Joint Reviews
LOG (xx-LOG-xxx)	Requirements originating from the team looking at Logical Networks implications and interactions
NMC (xx-NMC-xxx)	Requirements Generated by team looking at Network Control and Network Management implications and interactions
Sxx (xx-Sxx-xxx)	Requirements originating from the team looking at Security implications and interactions

Security Subsections Categorization (xx of the Sxx identifier):

SAU	Authentication
SAV	Availability
SCO	Confidentiality
SGE	General Security
SIN	Integrity
SMA	Management
SNR	Non-repudiation
STR	Traceability

4 Functional Requirements

The following tables capture the Functional Requirements for the Project MESA system.

4.1 Core Functional Requirements

Table 1 consists of the functional requirements that would apply to developing standards and specifications for a MESA system.

Table 1: Functional Requirements

Functional Req. ID No.	Functional Requirement Text	Associated Mesa SoR Sections	Associated User Seq IDs
FR-ASC-001	Authorized principals shall be able to add, modify, or create and store in real-time, via an application or service, new data in database(s), files and automated systems, needed to successfully execute the application or service.	MesaSoR.5.54	282
FR-ASC-002	Authorized principals shall be able to retrieve in real-time, via an application or service, any data from database(s), files and automated systems, needed to successfully execute the application or service, by the authorized principals.	MesaSoR.5.54	283
FR-ASC-003	Authorized principals shall be able to modify in real-time, via an application or service, any data in database(s), files and automated systems, needed to successfully execute the application or service, by the authorized principals.	MesaSoR.5.54	284
FR-ASC-004	Authorized principals shall be able to add, modify or delete in real-time, via an application or service, any data in database(s), files and automated systems, needed to be removed in order to successfully execute the application or service, by the authorized principals.	MesaSoR.5.54	285
FR-ASC-005	Authorized principals shall be able to monitor and control features and functions of remote devices such as robotic devices, unmanned units, including but not limited to, via an application or service.	MesaSoR.5.54	286
FR-ASC-006	The applications and services that involve database transactions, file downloads, file uploads, remote control, including but not limited to, shall function on the logical network, transparently to and irrespective of the different layer protocols of the logical network, below the application layer.	MesaSoR.5.54	287
FR-ASC-007	1. Applications and services shall be designed in such way that they can be distributed to allow access from any end user devices. 2. Interoperable Applications and services should have a well-defined subset of mandatory features.	MesaSoR.5.54	288
FR-ASC-008	The user access to applications and services (which may vary based on client and device type) should allow the applications and services to be clearly identifiable, easy to access, and available for use by any authorized user.	MesaSoR.5.54	289
FR-ASC-009	Applications and services provided by the home network should be available to users in a visited network, subject to user's SLA, authorization policies provisioned in both the visited network and the home network and the jurisdiction agreements, and while maintaining confidentiality and integrity, once a user has been authenticated.	MesaSoR.5.54	290
FR-ASC-010	Application and services provided by the visited network should be available to users in a visited network, subject to user's SLA, authorization policies provisioned in the visited network, and the jurisdiction agreements.	MesaSoR.5.54	291
FR-ASC-011	To allow the sharing of data between agencies, applications and services shall support data exchanges via direct connections and/or via intermediary logical network resources.	MesaSoR.5.54	292
FR-ASC-012	1. Application and services shall support the assignment of roles (e.g. administrator, manager, delegate, user), rights (e.g. scope of accessible information, priority, authorization levels) and responsibilities (e.g. obligations). 2. Roles, rights and responsibilities may be assigned to various principals (e.g. individual users, groups of users, or applications).	MesaSoR.5.54	293

Functional Req. ID No.	Functional Requirement Text	Associated Mesa SoR Sections	Associated User Seq IDs
FR-ASC-020	Any applications and services shall implement standards that include mechanisms for initiating requests towards other resources in the logical network, and accepting responses from the same and/or other resources in the logical network.	MesaSoR.5.58	307
FR-ASC-021	Any applications and services shall implement standards that include mechanisms for subscribing to external events produced in or transmitted by other resources in the logical network, and mechanisms that allow them to receive notifications of events they have subscribed to.	MesaSoR.5.58	308
FR-ASC-022	Applications and services should be able to adapt the manner in which information is presented, accepted and transmitted in either direction, by the capability of the device or system that the user has access to (e.g. data terminals, subscriber radio, computer equipment) and the portability of the device or system (e.g. vehicle-mounted or hand-held).	MesaSoR.5.58	309
FR-ASC-023	Access to applications and services shall be allowed only to authenticated users, authorized for the use for specific applications and services, and/or specific features of such applications and services.	MesaSoR.5.58	310
FR-ASC-024	Once authenticated, a user should be able to access other services for which he/she is authorized, without the need to re-authenticate.	MesaSoR.5.58	311
FR-ASC-040	Applications and services should be designed to allow devices and/or systems to use their maximum capabilities.	MesaSoR.5.52(b)	263
FR-ASC-041	The applications and services should include, where applicable, the capability to process and/or accept, transcode, and transmit data in different media formats (e.g. voice, infrared video, text) with low-latency, and provide the end-user with the best possible user experience when accepting from and/or presenting the data to the user.	MesaSoR.5.52(b)	264
FR-ASC-042	The applications and services should support peer-to-peer communications between resources in the logical network, including user-to-user communications, using a variety of media formats (e.g. voice, infrared video, text).	MesaSoR.5.52(b)	265
FR-ASC-043	Applications and services that initiate and/or accept transmission of data in multiple media formats, while taking advantage of broadcast/multicast capabilities, shall be available.	MesaSoR.5.52(b)	266
FR-ASC-044	Services should include the support for simultaneous instantiation and execution of applications that may access, process, present or transmit data in different media formats (voice, data, video), if the devices and systems they use have such capabilities.	MesaSoR.5.52(b)	267
FR-ASC-060	Applications and/or services should be able to access and use a device's local capability to indicate its geographical position, in order to be able to process, transmit and present the device's location to authorized principals.	MesaSoR.5.56	300
FR-ASC-061	Applications and services should be able to have a choice in obtaining a user's position from the user's device or from a central resource available in the logical network (a location server) or from a central resource in a different associated logical network.	MesaSoR.5.56	301
FR-ASC-062	Location based applications and/or services should allow end-users to register for (subscribe to) location information of other end-users.	MesaSoR.5.56	302
FR-ASC-063	Location based applications and/or services should include capabilities to determine and communicate a device's geographical location information, including altitude, and/or its relative position to identifiable points of reference, even in the case of an in-building located device deprived of access to satellite communications.	MesaSoR.5.56	303
FR-ASC-080	Application and services should facilitate user access to information, by using the device and logical network capabilities available at any given moment in time.	MesaSoR.5.30	45
FR-ASC-081	Application and services should support information store-and-forward (at any time on the local device, and, when on-net, in a different resource in the logical network), in order to handle situations in which information may not be able to immediately be transmitted to the destination (e.g. the transmitting or the receiving device is off-net).	MesaSoR.5.30	46
FR-ASC-082	Applications and services should support on demand retrieval of information that has been cached on the user's device for the user's consumption.	MesaSoR.5.30	47

Functional Req. ID No.	Functional Requirement Text	Associated Mesa SoR Sections	Associated User Seq IDs
FR-ASC-083	Applications and services should support retrieval of information that has been cached on a resource in the logical network, to support the case when the device the user is using was off-net, and is later reversing to an on-net situation.	MesaSoR.5.30	48
FR-ASC-084	Applications and services should be able to facilitate the advertisement of the presence, availability, and status of a user (e.g. in the midst of an action, in transit, in a communication exchange, in a meeting).	MesaSoR.5.30	49
FR-ASC-085	Applications and services should be able to discover the advertisement of the presence, availability and status of a user (e.g. in the midst of an action, in transit, in a communication exchange, in a meeting).	MesaSoR.5.30	50
FR-ASC-100	Application and services should use device and logical network capabilities of point-to-point and point-to-multipoint voice communications.	MesaSoR.5.32	55
FR-ASC-101	Applications and services that use point-to-multipoint communication capabilities should include features for control for an authorized principal, if several of the points that are taking part in the application or service are capable of initiating communications to other points (e.g. users). NOTE: This feature is the equivalent of a moderator in a meeting.	MesaSoR.5.32	56
FR-ASC-102	Applications and services that use point-to-point and/or point-to-multipoint communication capabilities should include features allowing an authorized principal to add and/or remove communication points to an existing group of communication points (e.g. users).	MesaSoR.5.32	57
FR-ASC-103	Applications and services that use point-to-point and/or point-to-multipoint communication capabilities should include features allowing a member of a group of communication points to indicate their availability to participate in communications.	MesaSoR.5.32	58
FR-ASC-104	Applications and services that use point-to-point and/or point-to-multipoint communication capabilities should include features allowing a member of a group of communication points to discover their availability of other members of the group to participate in communications.	MesaSoR.5.32	59
FR-ASC-105	Applications and services that use point-to-point and/or point-to-multipoint communication capabilities should include features allowing members of a group of communication points to initiate and use data transfer channels, simultaneous with their communication channels.	MesaSoR.5.32	60
FR-ASC-120	Applications and services should be able to detect and act upon the activation of a panic button (local panic button activation).	MesaSoR.5.52(a)	255
FR-ASC-121	Applications and services should be able to detect and act upon a notification triggered by the activation of a panic button that was activated from a device or resource in the logical network different than the device used in the execution of the application (remote panic button activation).	MesaSoR.5.52(a)	256
FR-ASC-122	Applications and services should be able to execute, without any user intervention, policy rules included in a policy associated with the activation of the panic activation button.	MesaSoR.5.52(a)	257
FR-ASC-123	The actions triggered by a Panic Button activation should be configurable to cover different possible situations. Note: Policy rules could be provided to include evaluation of condition and context, and execution of actions based on the results of the evaluation, such as re-prioritizing resources on the used device, relinquishing resources in the logical network that the application was using, saving and/or immediately relaying critical data cached, switching to different communication channels or from point-to-point to point-to-multipoint voice communication.	MesaSoR.5.52(a)	258
FR-ASC-140	Applications and services should rely on nationally or internationally mobile applications and services enabler recognized standards, wherever possible.	MesaSoR.5.4	110
FR-ASC-141	1. Applications should be developed independent of underlying layers protocols, while supporting multiple realizations depending on the specifics of the physical network they will be deployed on. 2. When multiple protocols are supported, the choice of the appropriate protocol should be based on optimizing the performance of the application, without end-user involvement.	MesaSoR.5.4	111