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

Technical Specification

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

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/chaircor/ETSI_support.asp

Contents

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-nnn (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-mulitpoint 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

Functional Req. ID No.	Functional Requirement Text	Associated Mesa SoR Sections	Associated User Seq IDs
FR-ASC-161	Application and services shall conform to the security policies and requirements imposed by the logical networks in which they perform, and/or by the entities that are involved in the service.	MesaSoR.5.45	187
FR-ASC-163	Enabling and disabling tracing capabilities at all tracing-capable MESA components should be supported.	MesaSoR.5.45	189
FR-ASC-164	Secure authorized applications shall be able to trigger service-level tracing, which will result in tracing being performed at all MESA components that the service is traversing, which have been previously enabled for tracing.	MesaSoR.5.45	190
FR-AWN-001	The AWN shall transport end user voice and data communications.	MesaSoR.5.29	32
FR-AWN-002	The AWN shall support IP-based data communications.	MesaSoR.5.29	33
		MesaSoR.5.8	364
FR-AWN-003	The AWN Core shall be able to interface to the JAN core network.	MesaSoR.5.29	34
FR-AWN-004	The AWN should be able to provide backhaul for the IAN when/if the JAN is unavailable.	MesaSoR.5.29	35
FR-AWN-005	The AWN shall interface to the IAN in a manner that is transparent to end user IP applications.	MesaSoR.5.25	30
FR-AWN-006	The AWN airlinks and the AWN core networks should support Public Safety QoS and SLA parameters, so that public safety applications are supported transparently and public safety users can be prioritized across all networks.	MesaSoR.5.25	31
FR-AWN-008	The AWN should be based on a nationally or internationally recognized wireless system standards and equipment.	MesaSoR.5.4	103
FR-EUD-001	The device shall be capable of authenticating itself in the logical network(s) being accessed.	MesaSoR.5.8	312
FR-EUD-002	The device shall be capable of authorizing the user in the logical network(s) being accessed.	MesaSoR.5.8	313
FR-EUD-003	The device shall not allow access to the capabilities to be supported without authentication and authorization.	MesaSoR.5.8	314
FR-EUD-005	The device shall be capable of identifying the core network of the logical network being accessed and operate accordingly.	MesaSoR.5.8	315
FR-EUD-006	The device shall be capable of accessing the services of external networks (such as, but not limited to: P25, TETRA, and AWN).	MesaSoR.5.8	316
FR-EUD-007	The device shall be capable of inter-working and interoperating with appropriate external networks (such as, but not limited to: P25, TETRA, and AWN).	MesaSoR.5.8	317
FR-EUD-008	The device shall be capable of interfacing with inter-working and interoperability nodes deployed in the network.	MesaSoR.5.8	318
FR-EUD-009	The device shall be capable of determining its geographical location. The accuracy should be within 1 meter, but shall be at least as accurate as existing E911 solutions.	MesaSoR.5.56	296
FR-EUD-010	The device shall provide its geographical position location information to the authorized location based services within the Project MESA system.	MesaSoR.5.56	297
FR-EUD-011	The device shall be capable of determining geographical position location information from associated networks for supporting the location based services.	MesaSoR.5.56	298
FR-EUD-012	The device shall be able to determine its location inside buildings along with the altitude component in future.	MesaSoR.5.56	299
FR-EUD-013	The device shall be able to access logical network(s) supported in the device.	MesaSoR.5.8	319
FR-EUD-014	The device shall be able to access services and applications supported by the accessible logical and external networks.	MesaSoR.5.30	40
FR-EUD-015	The device shall support point-to-point communications.	MesaSoR.5.32	52
FR-EUD-016	The device shall support point-to-multipoint communications.	MesaSoR.5.32	53
FR-EUD-017	The device shall provide the use with ability to declare panic situation.	MesaSoR.5.52(a)	251
FR-EUD-018	The device shall notify the service and/or network of panic situation declaration from the user.	MesaSoR.5.52(a)	253
FR-EUD-019	The device shall prioritize and manage the resources during the panic situation.	MesaSoR.5.52(a)	254
FR-EUD-022	The device shall be compliant to the regulations that apply to the physical network(s) being accessed.	MesaSoR.5.17	11
FR-EUD-024	The device shall comply with applicable and relevant emission limits for its band of operation.	MesaSoR.5.18	13
FR-EUD-026	The device shall comply with applicable RF safety regulations.	MesaSoR.5.18	16

Functional Req. ID No.	Functional Requirement Text	Associated Mesa SoR Sections	Associated User Seq IDs
FR-EUD-027	The device shall recognize transmission delays introduced in the network and treat the information according to determined classes of service.	MesaSoR.5.57	304
FR-EUD-028	The device shall be capable of accessing all services authorized to the user and upon successful authentication.	MesaSoR.5.8	320
FR-EUD-032	The device shall be able to establish a network with other peer devices and utilize services and applications available to that peer network.	MesaSoR.5.30	41
FR-EUD-036	The device shall be compliant to the regional safety standards such as European Commission or Underwriters Laboratory.	MesaSoR.5.18	17
FR-EUD-039	The device shall be able to select the most efficient logical network for communication and transparently switch to more effective logical network.	MesaSoR.5.8	321
FR-EUD-042	The device shall allow the user to select logical network access by overriding the automatic selection procedure.	MesaSoR.5.8	322
FR-EUD-043	The device shall support administration functions initiated by the network, end user or the device itself.	MesaSoR.5.8	323
FR-EUD-044	The device shall collect and report errors to the service or administration control.	MesaSoR.5.8	324
FR-IOP-001	The MESA systems shall use IP (Internet Protocol) as the common layer 3 interface. Physical and Link Layer interconnections between network components (excluding wireless components) shall be based on the 802.3 (Ethernet) standards.	MesaSoR.5.4	104
FR-IOP-003	The network must support the ability to add new infrastructure components (with minimal configuration or setup required) into the existing infrastructure and become operational with little to no configuration or setup required.	MesaSoR.5.7	327
FR-IOP-004	The network shall be capable of dynamically scaling to accommodate a growing number of users. This scaling shall not sacrifice any mission-critical services, applications or network functionality, and should not sacrifice any services, applications or network functionality.	MesaSoR.5.7	328
FR-IOP-005	Common layer 1-2 interface specifications shall be developed. If more than one such specification is implemented in a user device, the infrastructure must also accommodate multiple modes.	MesaSoR.5.9	365
FR-IOP-006	The common layer 1-2 interface shall allow for infrastructureless communications between user devices.	MesaSoR.5.9	366
FR-IOP-008	Project MESA specifications shall provide network interfaces to legacy systems that provide backwards compatibility between MESA devices and legacy devices.	MesaSoR.5.20	23
FR-IOP-009	Project MESA specifications must provide forward compatibility (including network components, applications and services, and devices used on the network).	MesaSoR.5.21	27
FR-IOP-010	Project MESA specifications shall provide a nonproprietary, publicly available interface through which non-Project MESA compliant systems can connect.	MesaSoR.5.21	28
FR-IOP-011	A public safety user shall be authenticated before accessing network resources.	MesaSoR.5.44	162
FR-IOP-012	A public safety user shall be able to authenticate from any portion of the network.	MesaSoR.5.44	163
FR-IOP-013	A public safety user shall be authorized to use specified network resources once authenticated.	MesaSoR.5.44	164
FR-IOP-014	A public safety user shall be able to gain authorization from any portion of the network.	MesaSoR.5.44	165
FR-IOP-015	Access to (seeing the contents of) traffic traversing the network or public safety segments of shared networks shall be limited to authorized recipients based upon their need and right to know.	MesaSoR.5.44	166
FR-IOP-016	The traffic traversing the network shall be immune to attacks against its integrity.	MesaSoR.5.44	167
FR-IOP-017	Authentication, authorization, and other security attributes shall be decoupled (independent of each other and the transport) such that a federated approach to security is possible.	MesaSoR.5.44	168
FR-IOP-018	Security specifications shall be capable of scaling to its appropriate context, i.e. local, county, state, regional, federal, etc., such that performance of the security specifications is not compromised.	MesaSoR.5.44	169
FR-JRA-001	The MESA system shall facilitate the sharing of spectrum with other radio technologies.	MesaSoR.5.15	7

Functional Req. ID No.	Functional Requirement Text	Associated Mesa SoR Sections	Associated User Seq IDs
FR-JRA-002	The MESA system shall provide data interoperability with data systems based on legacy public safety standards (such as, but not limited to: Tetra and P25).	MesaSoR.5.20	25
FR-JRA-003	The MESA system shall provide voice interoperability with voice systems based on legacy public safety standards (such as, but not limited to: Tetra and P25). Due to the mission critical nature of voice services on legacy systems, this interoperability cannot impede or negatively affect the voice services on the legacy networks.	MesaSoR.5.20	26
FR-JRA-004	The system shall be able to be configured such that user application data that is undelivered due to system connectivity issues (such as, but not limited to coverage holes and outages) can be cached and delivered when connectivity is restored.	MesaSoR.5.57	305
FR-JRA-005	The end user shall have access to all authorized services supported by the level of connectivity to the logical networks, both on-net and off-net.	MesaSoR.5.30	42
FR-JRA-006	The device may bridge authorized communications across logical networks. For example, a JAN communication may be relayed by a device with both JAN and Ad Hoc iAN peer to peer connectivity to another device that does not have JAN connectivity but does have Ad Hoc IAN connectivity.	MesaSoR.5.30	43
FR-JRA-007	The system shall only pre-empt if network conditions become so degraded as to affect the service.	MesaSoR.5.38	99
FR-JRA-009	The system shall provide mechanisms for authenticated and authorized users (such as an administrator or supervisor) to manage, clear and/or override the panic situation.	MesaSoR.5.52(a)	252
FR-JRA-010	The network's geographic coverage shall be able to scale efficiently and cost effectively.	MesaSoR.5.7	325
FR-JRA-011	The network shall be able to scale with usage efficiently and cost effectively.	MesaSoR.5.7	326
FR-JRA-012	The system should be capable for continuous operation at maximum utilization and maximum throughput.	MesaSoR.5.52	250
FR-JRA-013	The device specifications and compliance information should be available and linked with databases of devices in use in the network and allow authorized users to query compliance information for all devices under their control.	MesaSoR.5.18	15
FR-JRA-014	The device should have the ability to make available information that will allow retrieval of compliance and conformance information.	MesaSoR.5.18	19
FR-JRA-016	Services provided by the system shall be consistent throughout the coverage area, including in-building and in-vehicle.	MesaSoR.5.10	3
FR-JRA-017	The system and its components shall allow for single service dedicated sessions as well as multiple simultaneous service sessions.	MesaSoR.5.31	51
FR-LOG-001	The logical network being accessed shall authenticate the device prior to allowing use of network services requiring such authentication.	MesaSoR.5.50	229
FR-LOG-001	The logical network being accessed shall authenticate the device prior to allowing use of network services requiring such authentication.	MesaSoR.5.7	329
FR-LOG-002	The logical network being accessed shall authorize the end user prior to allowing use of network services requiring such authorization.	MesaSoR.5.50	230
FR-LOG-002	The logical network being accessed shall authorize the end user prior to allowing use of network services requiring such authorization.	MesaSoR.5.7	330
FR-LOG-003	The logical network shall re-authenticate the device prior to allowing use of network services requiring such authentication when the device is being transparently transferred to a different logical network.	MesaSoR.5.50	231
FR-LOG-003	The logical network shall re-authenticate the device prior to allowing use of network services requiring such authentication when the device is being transparently transferred to a different logical network.	MesaSoR.5.7	331
FR-LOG-004	The logical network shall reauthorize the end user prior to allowing use of network services requiring such authorization when the device is being transparently transferred to a different logical network.	MesaSoR.5.7	332
FR-LOG-004	The logical network shall reauthorize the end user prior to allowing use of network services requiring such authorization when the device is being transparently transferred to a different logical network.	MesaSoR.5.50	232
FR-LOG-005	The logical network shall allow authorized users access to authorized database(s) in real-time.	MesaSoR.5.54	275
FR-LOG-006	The logical network shall allow authorized users access to modify specified authorized database(s) in real-time.	MesaSoR.5.54	276

Functional Req. ID No.	Functional Requirement Text	Associated Mesa SoR Sections	Associated User Seq IDs
FR-LOG-007	The logical network shall allow the user access to monitor and control features and functions of remote devices such as, but not limited to, robotic devices and unmanned units.	MesaSoR.5.54	277
FR-LOG-008	The logical network shall allow authorized users access to automated systems and files.	MesaSoR.5.54	278
FR-LOG-010	The logical network(s) being accessed shall include transparent interfaces such that the user services rendered are uniform across logical networks.	MesaSoR.5.29	36
FR-LOG-012	The logical network(s) shall support access from users belonging to multiple agencies.	MesaSoR.5.7	333
FR-LOG-013	The logical network(s) shall support access to multiple services from users.	MesaSoR.5.7	334
FR-LOG-014	The logical network(s) shall support access to multiple network functions by device clients.	MesaSoR.5.7	335
FR-LOG-016	The logical network(s) shall provide simultaneous access to multiple applications (e.g. host computer) from the same user.	MesaSoR.5.37	92
FR-LOG-017	The logical network(s) shall provide simultaneous access to multiple users to the same application (e.g. host computer).	MesaSoR.5.37	93
FR-LOG-018	The logical network(s) shall support simultaneous transfer of voice and data between user and services platforms.	MesaSoR.5.52(b)	259
FR-LOG-019	The logical network(s) shall support simultaneous transfer of voice and data between users.	MesaSoR.5.52(b)	260
FR-LOG-020	The logical network(s) shall transparently support application layer protocols, such as (but not limited to) data base transactions, file download, file uploads, and remote control.	MesaSoR.5.54	279
		MesaSoR.5.29	37
FR-LOG-021	The logical network(s) shall support the capability to interface with external services belonging to multiple agencies.	MesaSoR.5.7	336
FR-LOG-028	The logical network(s) being accessed shall be capable of interfacing with inter-working and interoperability nodes deployed in the network.	MesaSoR.5.7	337
FR-LOG-029	The logical network(s) being accessed shall be capable of inter-working and interoperation with external networks (such as, but not limited to, AWN, P25, and TETRA). Interoperating should be a configuration option.	MesaSoR.5.7	338
FR-LOG-030	The public safety network shall accommodate logical networks as defined in the Public Safety Network - High Level Architecture.	MesaSoR.5.7	339
FR-LOG-031	The logical network(s) shall support access to on-net services and applications.	MesaSoR.5.30	44
FR-LOG-037	The logical network(s) shall allow access to services and applications from all properly authenticated and authorized devices and end users.	MesaSoR.5.7	340
FR-LOG-038	The logical network(s) shall support multicast/broadcast to the users.	MesaSoR.5.52(b)	261
FR-LOG-040	The logical network(s) shall support interfaces to multiple radio access networks (which may be the same or different technologies).	MesaSoR.5.29	38
		MesaSoR.5.7	341
FR-LOG-042	The logical network(s) shall provide seamless operation of services and applications between radio interfaces.	MesaSoR.5.7	342
FR-LOG-043	Interfaces between logical networks shall use existing standardized protocols and utilize COTS technology.	MesaSoR.5.4	105
FR-LOG-044	The logical network(s) shall provide seamless operation of services and applications.	MesaSoR.5.4	106
FR-LOG-045	Seamless operation shall be possible across logical network boundaries.	MesaSoR.5.4	107
FR-LOG-048	The logical network(s) shall provide seamless operation of services and applications when transferring between nodes in the same network or across networks.	MesaSoR.5.50	233
FR-LOG-049	The logical network(s) shall not permit the transfers if restricted by user profile.	MesaSoR.5.50	234
FR-LOG-050	The logical network(s) shall support interoperability among the users accessing different logical network(s).	MesaSoR.5.9	367
FR-LOG-051	The logical network(s) shall allow access to home subscribers of other networks based on the user profile.	MesaSoR.5.9	368
FR-LOG-052	The logical network(s) shall allow user access as per the user profile.	MesaSoR.5.7	343
FR-LOG-053	The logical network(s) shall support priority access based on user profile.	MesaSoR.5.7	344
FR-LOG-054	The logical network(s) shall support real time resource management functions, such as (but not limited to) radio and network resource allocation, system configurations and user configurations.	MesaSoR.5.7	345

Functional Req. ID No.	Functional Requirement Text	Associated Mesa SoR Sections	Associated User Seq IDs
FR-NMC-002	The system shall transparently support application layer protocols and packets.	MesaSoR.5.54	281
FR-NMC-002	The system shall transparently support application layer protocols and packets.	MesaSoR.5.53	268
FR-NMC-003	The system shall permit the field application to dynamically request/change QoS.	MesaSoR.5.34	68
FR-NMC-004	The system shall permit the network administrator to dynamically request/change QoS.	MesaSoR.5.34	69
FR-NMC-005	The system shall permit the network administrator to dynamically - automatic or manually - configure application access to QoS.	MesaSoR.5.34	70
FR-NMC-006	The system shall support the configuration and re-configuration of the QoS attributes including minimum bit rate, maximum bit rate, maximum SDU size and service class as examples.	MesaSoR.5.34	71
FR-NMC-007	The system shall support adaptive coding to maximize the aggregate user throughput, and to ensure individual users are able to maximize their throughput for their given channel conditions.	MesaSoR.5.15	5
FR-NMC-008	The system shall provide configuration options that allow redundancy for critical network components.	MesaSoR.5.48	223
FR-NMC-008	The system shall provide configuration options that allow redundancy for critical network components.	MesaSoR.5.51	246
FR-NMC-010	The system shall support the channel configuration that utilizes all the bandwidth allocated.	MesaSoR.5.15	6
FR-NMC-013	The system shall support user/agency-based features including but not limited to group priority, group security policy, roaming authorization and transmission power.	MesaSoR.5.33	61
FR-NMC-014	The system shall support bandwidth partitioning at a site to various user groups.	MesaSoR.5.33	62
FR-NMC-015	The system shall grant/reject the QoS based upon user's authorized services and priority.	MesaSoR.5.34	73
FR-NMC-016	The system shall support at least as many classes of service as existing LMR systems.	MesaSoR.5.35	78
FR-NMC-017	The system shall support QoS for different classes of service.	MesaSoR.5.35	79
FR-NMC-018	The system shall support independent QoS flows for different classes of service.	MesaSoR.5.35	80
FR-NMC-020	The system shall provide the ability for network administrators to assign authorized service classes to users and user groups.	MesaSoR.5.35	82
FR-NMC-021	The system shall support different levels of service priorities.	MesaSoR.5.36	85
FR-NMC-023	The network management system shall allow the configuration of user priorities.	MesaSoR.5.36	86
FR-NMC-024	Priority should be applied system-wide such that it is recognized globally, but enforced locally based upon local policies. Priority parameters should not be limited to specific user groups (agencies, jurisdictions, private or commercial networks) so that the appropriate enforcement of priority can be accomplished (which nominally entails public safety entities having priority over non-public safety entities).	MesaSoR.5.36	87
FR-NMC-025	The network management system shall permit the assigning of the highest level of priority to public safety users.	MesaSoR.5.36	88
FR-NMC-026	The system shall prioritize network access based upon classes of service and user priorities.	MesaSoR.5.38	97
FR-NMC-027	The system shall support pre-emption based upon service and user priorities.	MesaSoR.5.38	98
		MesaSoR.5.34	74
FR-NMC-028	The system shall provide error detection and correction methods.	MesaSoR.5.48	224
FR-NMC-029	The system should support seamless user and service mobility independent of the radio access networks.	MesaSoR.5.9	369
		MesaSoR.5.4	108
		MesaSoR.5.50	235
FR-NMC-030	The system shall support seamless user and service mobility across different core networks.	MesaSoR.5.50	237
		MesaSoR.5.4	109
		MesaSoR.5.9	370
FR-NMC-034	The system should be designed to support real-time and other high performance services. For voice communications, the end-to-end delay should not exceed 150 ms for duplex systems and 250 ms for half-duplex systems. For links involving a non-terrestrial node, the delay shall not exceed 400 ms.	MesaSoR.5.48	225

Functional Req. ID No.	Functional Requirement Text	Associated Mesa SoR Sections	Associated User Seq IDs
FR-NMC-034	The system should be designed to support real-time and other high performance services. For voice communications, the end-to-end delay should not exceed 150 ms for duplex systems and 250 ms for half-duplex systems. For links involving a non-terrestrial node, the delay shall not exceed 400 ms.	MesaSoR.5.53	269
FR-NMC-034	The system should be designed to support real-time and other high performance services. For voice communications, the end-to-end delay should not exceed 150 ms for duplex systems and 250 ms for half-duplex systems. For links involving a non-terrestrial node, the delay shall not exceed 400 ms.	MesaSoR.5.55	294
FR-NMC-034	The system should be designed to support real-time and other high performance services. For voice communications, the end-to-end delay should not exceed 150 ms for duplex systems and 250 ms for half-duplex systems. For links involving a non-terrestrial node, the delay shall not exceed 400 ms.	MesaSoR.5.49	227
FR-NMC-035	The system shall support location based applications.	MesaSoR.5.53	270
FR-NMC-036	The system should be able to provide sufficient resources to prioritized applications.	MesaSoR.5.53	271
FR-NMC-036	The system should be able to provide sufficient resources to prioritized applications.	MesaSoR.5.55	295
FR-NMC-037	The system shall support customer specific applications running on the application layer of the network.	MesaSoR.5.53	272
FR-NMC-040	The radio network of the system shall have mechanisms to minimize the interference to adjacent systems and/or channels to a level that conforms to regulatory guidelines or specifications, or conforms with criteria specified in agreed to service level agreements, whichever is the more stringent standard.	MesaSoR.5.19	20
FR-NMC-041	The radio network of the system shall have mechanisms to minimize the effect of interference from adjacent systems and/or channels such that operations of MESA services are uninterrupted.	MesaSoR.5.19	21
FR-NMC-044	The system shall permit the dynamic request/change of QoS.	MesaSoR.5.34	75
FR-NMC-045	The system shall allow public safety users to have the highest level of priority.	MesaSoR.5.36	89
FR-NMC-046	The system shall be able to provide services to in-vehicle subscribers.	MesaSoR.5.10	1
FR-NMC-047	The system shall be able to provide services to in-building subscribers.	MesaSoR.5.10	2
FR-NMC-048	The system shall support location-based configuration profiles for end users and devices. NOTE: This capability would allow for services to vary depending on geographical scales. For example, a multi-jurisdictional JAN where users and devices in one portion of the JAN have access to a suite of services and policies, and when those users or devices move to a different portion, they have a different set of services and policies.	MesaSoR.5.9	372
FR-NMC-048	The system shall support location-based configuration profiles for end users and devices. NOTE: This capability would allow for services to vary depending on geographical scales. For example, a multi-jurisdictional JAN where users and devices in one portion of the JAN have access to a suite of services and policies, and when those users or devices move to a different portion, they have a different set of services and policies.	MesaSoR.5.8	371
FR-NMC-050	The system shall prioritize QoS resource reservations based on user priority.	MesaSoR.5.38	101
FR-NMC-051	The system shall allow the network administrator to create, configure, and remove user groups.	MesaSoR.5.33	63
FR-NMC-052	The system shall allow the network administrator to add/delete users to/from a user group at run-time.	MesaSoR.5.33	64
FR-NMC-053	The system shall allow the network administrator to configure user group parameters including but not limited to group priority, group security policy, roaming authorization and transmission power.	MesaSoR.5.33	65
FR-NMC-054	The system shall allow the network administrator to partition the bandwidth at a site to various user groups.	MesaSoR.5.33	66
FR-NMC-055	The network management system shall allow each user group (agency/jurisdiction) to manage their own network resources and user configurations.	MesaSoR.5.33	67

Functional Req. ID No.	Functional Requirement Text	Associated Mesa SoR Sections	Associated User Seq IDs
FR-NMC-056	The system shall report failures of all network components.	MesaSoR.5.51	247
FR-NMC-057	The system shall automatically push network configurations to backup network components.	MesaSoR.5.51	248
FR-NMC-058	The system shall allow authorized and secure access to authentication transactions (system messages relating to authentication state) in real time.	MesaSoR.5.40	112
FR-NMC-059	The system shall allow authorized and secure access to authorization transactions (system messages relating to authorization state) in real time.	MesaSoR.5.40	114
FR-NMC-060	The system shall allow authorized and secure access to authentication records (current authentication state).	MesaSoR.5.40	116
FR-NMC-061	Authorization and authentication transactions and record information accessed shall be non-repudiative.	MesaSoR.5.40	118
FR-NMC-062	The system shall assist the network manager in creating an audit trail by maintaining data in a common format.	MesaSoR.5.40	120
FR-NMC-064	The system shall support standard network management protocols.	MesaSoR.5.41	136
FR-NMC-065	The network management system shall support the generation of system resource usage reports (e.g. system resource utilization reports) for each subscriber and for each user group.	MesaSoR.5.41	137
FR-NMC-065	The network management system shall support the generation of system resource usage reports (e.g. system resource utilization reports) for each subscriber and for each user group.	MesaSoR.5.42	146
FR-NMC-066	The network management system shall support the generation of traffic pattern reports.	MesaSoR.5.41	138
FR-NMC-066	The network management system shall support the generation of traffic pattern reports.	MesaSoR.5.42	147
FR-NMC-067	The network management system shall support the generation of performance reports of the system and its components.	MesaSoR.5.42	148
FR-NMC-067	The network management system shall support the generation of performance reports of the system and its components.	MesaSoR.5.41	139
FR-NMC-068	The network management system and all of its data shall be protected from unauthorized access.	MesaSoR.5.41	140
FR-NMC-069	The system shall only allow access by authorized users.	MesaSoR.5.46	191
FR-NMC-070	The system shall only allow access by authorized devices.	MesaSoR.5.46	192
FR-NMC-071	The system shall be able to disable and enable the access by specific users.	MesaSoR.5.46	193
FR-NMC-072	The system shall be able to disable specific users at run-time.	MesaSoR.5.46	194
FR-NMC-073	The system shall be able to disable and enable the access by specific devices.	MesaSoR.5.46	195
FR-NMC-074	The system shall be able to disable specific devices at run-time.	MesaSoR.5.46	196
FR-NMC-075	The system shall support over the air rekeying.	MesaSoR.5.47	203
FR-NMC-076	The system should transparently support the applications that automatically update data fields being transmitted from user devices.	MesaSoR.5.58	306
FR-NMC-077	The system shall ensure service classes assigned to users and user groups are enforced throughout the MESA system, end to end.	MesaSoR.5.35	83
FR-NMC-078	The network management system shall allow authorized network managers to modify user priorities which are implemented immediately upon change.	MesaSoR.5.36	90
FR-NMC-079	The system shall keep track of the status history of all system components.	MesaSoR.5.40	123
FR-NMC-080	The system shall have the capability to keep track of all QoS operational and configuration transactions.	MesaSoR.5.40	124
FR-NMC-081	The system shall allow authorized network managers access to status history of system components.	MesaSoR.5.40	125
FR-NMC-083	The network management system shall be able to automatically discover the network components of the system.	MesaSoR.5.43	153
FR-NMC-084	The network management system shall be able to automatically discover the user devices.	MesaSoR.5.43	154
FR-NMC-085	The auto-discovery protocol used by network management system shall be protected from unauthorized access.	MesaSoR.5.43	155
FR-NMC-086	Network management packets shall be encrypted.	MesaSoR.5.40	127
FR-NMC-087	The network management system shall support the generation of reports on unauthorized network access attempts.	MesaSoR.5.41	141
FR-NMC-089	The radio network of the system shall transparently support the protocols used by the core network of the system.	MesaSoR.5.29	39

Functional Req. ID No.	Functional Requirement Text	Associated Mesa SoR Sections	Associated User Seq IDs
FR-NMC-090	The system shall automatically bring up backup components to provide service upon failures of primary network component.	MesaSoR.5.51	249
FR-NMC-091	The system shall manage and monitor network resources and grant/reject the QoS flows based upon user's authorized services and priority.	MesaSoR.5.34	76
FR-NMC-092	The system shall grant service only to authorized users and user groups.	MesaSoR.5.35	84
FR-NMC-093	The system shall provide service on a "first-in - first-out" basis within each priority class.	MesaSoR.5.39	102
FR-NMC-094	The user device of the system should be able to simultaneously access multiple networks.	MesaSoR.5.9	363
		MesaSoR.5.37	94
FR-NMC-095	The user device of the system should be able to simultaneously access multiple host computers.	MesaSoR.5.37	95
FR-NMC-096	The host computer of the system shall allow simultaneous access from multiple user devices.	MesaSoR.5.37	96
FR-NMC-098	The system shall support point-to-multipoint communications.	MesaSoR.5.32	54
		MesaSoR.5.52(b)	262
FR-NMC-100	The system shall monitor and control the bandwidth usage to their granted limit.	MesaSoR.5.34	77
FR-NMC-102	The system should be deployable in any valid allocated frequency band or bands.	MesaSoR.5.14	4
FR-NMC-103	The system shall allow authorized and secure access to a historical log of authentication transactions.	MesaSoR.5.40	113
FR-NMC-104	The system shall allow authorized and secure access to a historical log of authorization transactions.	MesaSoR.5.40	115
FR-NMC-105	The system shall allow authorized and secure access to authorization records (current authorization state).	MesaSoR.5.40	117
FR-NMC-110	Within the available spectrum, the system shall support dynamic air interface transfer rates to enable communications to efficiently operate under dynamic radio conditions.	MesaSoR.5.34	72
FR-SAU-001	All devices shall carry an unalterable unique ID and provide the ability for an authorized administrator to assign a separate ID, which can only be altered by an authorized administrator.	MesaSoR.5.44	170
FR-SAU-001	All devices shall carry an unalterable unique ID and provide the ability for an authorized administrator to assign a separate ID, which can only be altered by an authorized administrator.	MesaSoR.5.46	197
FR-SAU-001	All devices shall carry an unalterable unique ID and provide the ability for an authorized administrator to assign a separate ID, which can only be altered by an authorized administrator.	MesaSoR.5.43	156
FR-SAU-001	All devices shall carry an unalterable unique ID and provide the ability for an authorized administrator to assign a separate ID, which can only be altered by an authorized administrator.	MesaSoR.5.47	204
FR-SAU-001	All devices shall carry an unalterable unique ID and provide the ability for an authorized administrator to assign a separate ID, which can only be altered by an authorized administrator.	MesaSoR.5.7	346
FR-SAU-002	All MESA users shall have a unique identifier that is independent of other identifiers (such as device), such that the system can distinguish the user as a distinct entity.	MesaSoR.5.43	157
FR-SAU-002	All MESA users shall have a unique identifier that is independent of other identifiers (such as device), such that the system can distinguish the user as a distinct entity.	MesaSoR.5.7	347
FR-SAU-002	All MESA users shall have a unique identifier that is independent of other identifiers (such as device), such that the system can distinguish the user as a distinct entity.	MesaSoR.5.46	198
FR-SAU-002	All MESA users shall have a unique identifier that is independent of other identifiers (such as device), such that the system can distinguish the user as a distinct entity.	MesaSoR.5.47	205
FR-SAU-002	All MESA users shall have a unique identifier that is independent of other identifiers (such as device), such that the system can distinguish the user as a distinct entity.	MesaSoR.5.44	171
FR-SAU-003	The system and user shall mutually authenticate before access.	MesaSoR.5.40	128
		MesaSoR.5.50	239
		MesaSoR.5.47	206
		MesaSoR.5.44	172
		MesaSoR.5.7	348

Functional Req. ID No.	Functional Requirement Text	Associated Mesa SoR Sections	Associated User Seq IDs
		MesaSoR.5.46	199
FR-SAU-004	The system shall make single sign-on available, and it should be utilized by applications and services. Some applications and services may require additional authentication and authorization beyond that provided by the single sign on service.	MesaSoR.5.50	240
		MesaSoR.5.7	349
		MesaSoR.5.47	207
		MesaSoR.5.40	129
		MesaSoR.5.44	173
FR-SAU-005	Every management operation shall be logged and be traceable to the specific individual or entity initiating the management operation.	MesaSoR.5.42	149
		MesaSoR.5.46	200
		MesaSoR.5.41	142
		MesaSoR.5.44	174
		MesaSoR.5.7	350
		MesaSoR.5.40	130
		MesaSoR.5.47	208
FR-SAU-006	Users shall be assigned a means for permissive and revocable proof of id (such as an electronic certificate).	MesaSoR.5.7	351
		MesaSoR.5.44	175
		MesaSoR.5.50	241
		MesaSoR.5.47	209
FR-SAU-007	All devices shall be authenticated, and authorized for any non-user specific applications, services or functionality available and authorized for that device.	MesaSoR.5.44	176
		MesaSoR.5.7	352
		MesaSoR.5.50	242
		MesaSoR.5.47	210
FR-SAU-008	All usage of MESA services shall be governed by security profiles.	MesaSoR.5.7	353
		MesaSoR.5.44	177
		MesaSoR.5.47	211
		MesaSoR.5.40	131
		MesaSoR.5.45	182
FR-SAV-001	All important data in a MESA system shall be stored such that 100% availability is maintained. A single failure shall not affect data availability. All MESA systems shall be error resilient, fail-safe, and mistake forgiving.	MesaSoR.5.44	178
		MesaSoR.5.47	212
FR-SAV-002	The MESA system shall deliver application data within the error performance criteria of the application.	MesaSoR.5.53	273
FR-SCO-001	It shall be possible to transfer data without unauthorized disclosure of its contents.	MesaSoR.5.7	354
		MesaSoR.5.40	132
		MesaSoR.5.47	213
		MesaSoR.5.44	179
		MesaSoR.5.42	150
		MesaSoR.5.41	143
FR-SGE-002	Implementation of MESA components shall allow configuration of how untrusted connections ought to be treated. Note: Untrusted connections are those where the connecting parties have not conducted prior mutual authentication and authorization.	MesaSoR.5.20	24
FR-SGE-003	Implementation of MESA components shall be compatible with previous MESA specifications.	MesaSoR.5.21	29
FR-SIN-001	It shall be possible to transfer data protected from change.	MesaSoR.5.42	151
		MesaSoR.5.7	355
		MesaSoR.5.47	214
		MesaSoR.5.44	180
		MesaSoR.5.41	144
		MesaSoR.5.53	274
		MesaSoR.5.40	133
FR-SMA-001	Device IDs (examples: device status, revocation lists) shall be maintained in secure, highly available, recoverable databases under the operational control of the local administrator(s) of the devices.	MesaSoR.5.47	215
		MesaSoR.5.7	356
		MesaSoR.5.50	243
		MesaSoR.5.46	201
		MesaSoR.5.43	158
FR-SMA-002	User IDs (examples: device status, revocation lists) shall be maintained in secure, highly available, recoverable databases under the operational control of the local administrator(s) of the users.	MesaSoR.5.50	244
		MesaSoR.5.43	159
		MesaSoR.5.47	216
		MesaSoR.5.46	202
		MesaSoR.5.7	357
FR-SMA-003	Inter-agency communication shall be governed by security profiles and non-repudiative user and device authentication.	MesaSoR.5.7	358
		MesaSoR.5.45	183
		MesaSoR.5.50	245

Functional Req. ID No.	Functional Requirement Text	Associated Mesa SoR Sections	Associated User Seq IDs
		MesaSoR.5.47	217
FR-SMA-004	Crypto keys shall be possible to be managed remotely.	MesaSoR.5.47	218
FR-SNR-001	It shall be possible to make non-repudiative transactions, both sending and receiving. These transactions can be user based, device based, application/service based, or network based.	MesaSoR.5.44	181
		MesaSoR.5.45	184
		MesaSoR.5.40	134
		MesaSoR.5.47	219
		MesaSoR.5.7	359
FR-STR-001	The system shall make available to authorized applications or services all users involved in a communication transaction/session.	MesaSoR.5.43	160
		MesaSoR.5.47	220
		MesaSoR.5.7	360
FR-STR-002	The system shall make available to authorized applications or services all devices involved in a communication transaction/session.	MesaSoR.5.7	361
		MesaSoR.5.47	221
		MesaSoR.5.43	161
FR-STR-003	It shall be possible to trace transactions from source to destination across MESA components.	MesaSoR.5.41	145
		MesaSoR.5.40	135
		MesaSoR.5.42	152
		MesaSoR.5.7	362
		MesaSoR.5.47	222
		MesaSoR.5.45	185

4.2 Other Requirements

Table 2 consists of other requirements that were identified and are applicable to a MESA system, but do directly apply to the standards development phase.

Table 2: Other Requirements

Functional Req. ID No.	Functional Requirement Text	Associated Mesa SoR Sections	Associated User Seq IDs
DC-EUD-020	The device shall be ergonomically designed for use in environments specified in relevant specifications.	MesaSoR.5.17	9
DC-EUD-021	The device shall be user friendly to operate in these environmental conditions specified in relevant specifications.	MesaSoR.5.17	10
DC-EUD-023	The device shall meet relevant specifications that address operability by the users with special needs.	MesaSoR.5.17	12
DC-NMC-032	All outdoor devices in the system should be ruggedized.	MesaSoR.5.48	226
DR-EUD-025	The device specifications shall include inband, out of band, and spurious emissions, non-ionizing radiation exposure, and maximum audio levels. The specifications shall be made available to authorized users and agencies.	MesaSoR.5.18	14
DR-EUD-037	The device specifications shall include the compliance information.	MesaSoR.5.18	18
DR-IOP-007	A well-defined migration path should be created for legacy systems to migrate toward a network satisfying the requirements in the present document.	MesaSoR.5.20	22

History

Document history		
V3.1.1	February 2009	Publication