ETSI TR 103 585 V1.2.1 (2019-11)

Reconfigurable Radio Systems (RRS);
Radio Equipment (RE) reconfiguration use cases

Reference
RTR/RRS-0220

Keywords
software, use case

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://ipr.etsi.org/).

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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Reconfigurable Radio Systems (RRS).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The present document provides use cases for radio equipment reconfiguration through software. It extends the use cases defined in ETSI TR 103 062 [i.7] for mobile device reconfiguration to the more generic framework of radio equipment reconfiguration.

1 Scope

The scope of the present document is to define use cases for radio equipment reconfiguration through software.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI EN 302 969 (V1.2.1): "Reconfigurable Radio Systems (RRS); Radio Reconfiguration related Requirements for Mobile Devices".

[i.2] ETSI EN 303 095 (V1.2.1): "Reconfigurable Radio Systems (RRS); Radio Reconfiguration related Architecture for Mobile Devices".

[i.3] ETSI EN 303 146-1 (V1.2.1): "Reconfigurable Radio Systems (RRS); Mobile Device Information Models and Protocols; Part 1: Multiradio Interface (MURI)".

[i.4] ETSI EN 303 146-2 (V1.2.1): "Reconfigurable Radio Systems (RRS); Mobile Device (MD) information models and protocols; Part 2: Reconfigurable Radio Frequency Interface (RRFI)".

[i.5] ETSI EN 303 146-3 (V1.2.1): "Reconfigurable Radio Systems (RRS); Mobile Device (MD) information models and protocols; Part 3: Unified Radio Application Interface (URAI)".

[i.6] ETSI EN 303 146-4 (V1.1.2): "Reconfigurable Radio Systems (RRS); Mobile Device (MD) information models and protocols; Part 4: Radio Programming Interface (RPI)".

[i.7] ETSI TR 103 062 (V1.1.1): "Reconfigurable Radio Systems (RRS); Use Cases and Scenarios for Software Defined Radio (SDR) Reference Architecture for Mobile Device".

[i.8] Recommendation ITU-R S.1709-1: "Technical characteristics of air interfaces for global broadband satellite systems".

[i.9] From "Bent Pipes" to "Software Defined Payloads": Evolution and Trends of Satellite Communications Systems, Piero Angeletti, Riccardo De Gaudenzi and Marco Lisi, June, 2008.

[i.10] IETF RFC 7426: "Software-Defined Networking (SDN): Layers and Architecture Terminology".

[i.11] ETSI GS NFV 002 (V1.1.1): "Network Functions Virtualisation (NFV); Architectural Framework".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

FFT	Fast Fourier Transform
FPGA	Field Programmable Gate Array
GEO	Geostationary Earth Orbit
IoT	Internet of Things
LEO	Low Earth Orbit
LLC	Logic Link Control
MURI	Multi Radio Interface
NR	New Radio
RA	Radio Application
RadioApps	Radio Application Store
RAP	Radio Application Package
RAT	Radio Access Technology
RLC	Radio Link Control
RRS	Reconfigurable Radio Systems
SCC	Satellite Control Center
SDR	Software Defined Radio
SW	SoftWare
USB	Universal Serial Bus
V2X	Vehicle to Everything
RF	Radio Frequency
RX	Receive
TX	Transmit

4 Radio Equipment Reconfiguration Use Cases

4.1 Overview

This clause provides some use cases of the SW reconfiguration and related equipment-specific application scenarios. Use cases considered in this clause are as follows:

- Use Case "Smartphone Radio Reconfiguration" in clause 4.2.
- Use Case "Connected Vehicle Radio Reconfiguration" in clause 4.3.
- Use Case "Network Radio Reconfiguration" in clause 4.4.
- Use Case "IoT Device Reconfiguration" in clause 4.5.
- Use Case "Radio Reconfiguration through an external Component" in clause 4.6.
- Use Case "Reconfigurable Satellite Telecom Payload" in clause 4.7.

- Use Case "Bug-fix and security updates" in clause 4.8.

NOTE: Use Cases given in clauses 4.2, 4.3, 4.4, 4.5, 4.6 and 4.7 are design Use Cases; the Use Case given in clause 4.8 is a Use Case for achieving a defined purpose.

4.2 Use Case "Smartphone Radio Reconfiguration"

4.2.0 General

The average lifetime of smartphones is substantially shorter (~2 years) compared to other radio equipment (> 2 years) such as vehicles, base stations, etc. Since smartphones are also generic computing platforms, they are subject to gradual obsolescence - in terms of computing power - when new use cases and software-based solutions become available. Therefore, radio reconfiguration use cases corresponding to the evolution of communication standards do not seem to be a major factor in the case of smartphones. Rather, the scenario of optimizing the operation of smartphones in accordance to the functional blocks in a given Radio Application code that might be downloaded from RadioApp Stores will be the main factor determining the use case of the smartphone radio reconfiguration. In this context however, minor updates to Radio Applications remain critical in order to provide technical corrections and address security vulnerabilities. RadioApps, provided as the ETSI SW Reconfiguration solutions, extend or modify existing radio features and define solutions for technical, certification and security needs.

4.2.1 Scenario "Optimize the operation of Smartphone"

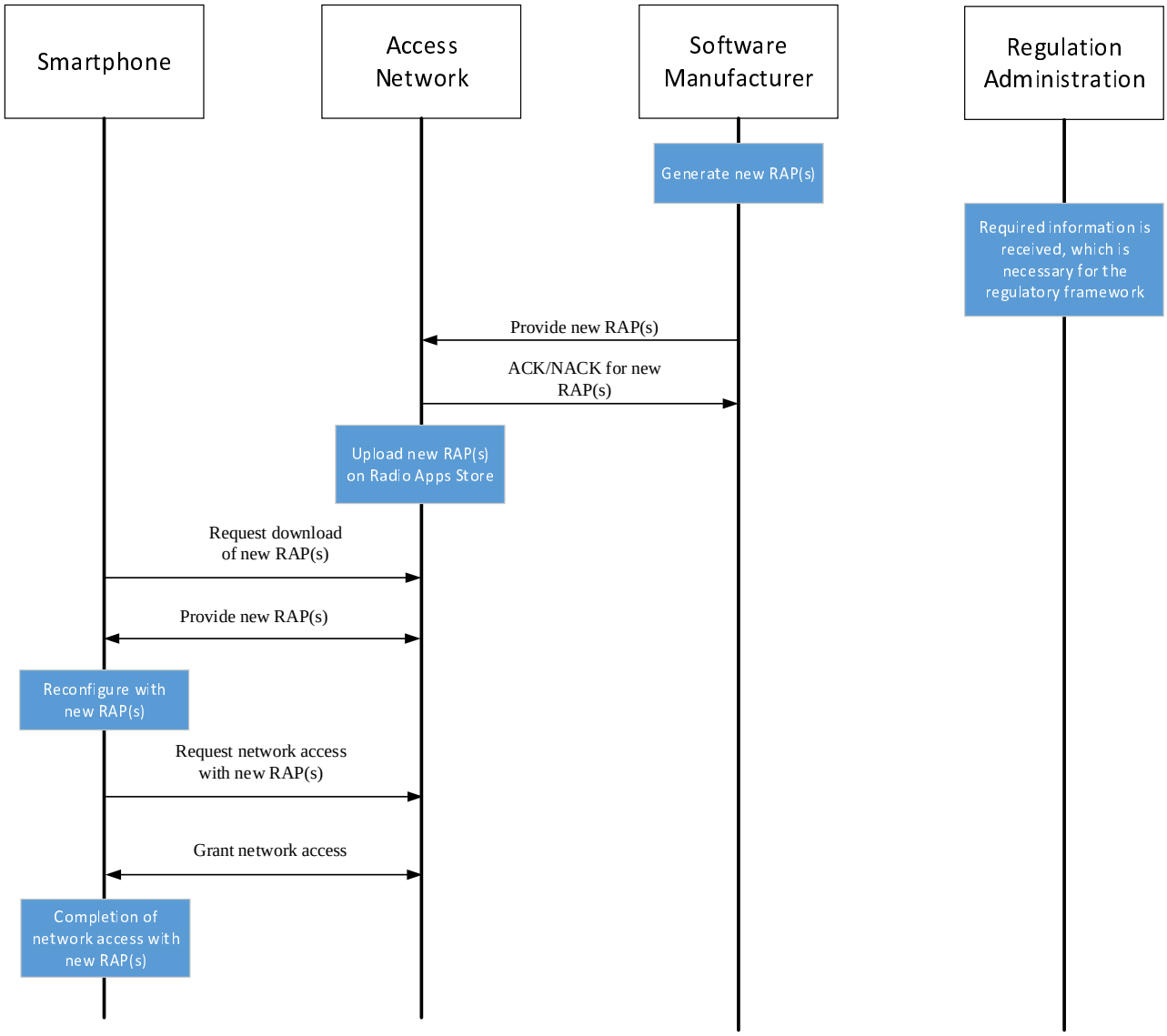
In this scenario, the operation of smartphone is optimized using an RA code corresponding to the required functional block(s) of desired communication protocol(s) downloaded from RadioApp Store upon user's request. For example, a LTE smartphone user could update his/her RA code of LTE protocol with a new FFT functional block which, for instance, utilizes less computational resources compared to the FFT functional block in the given RA code in order to save the computational complexity. The optimization of smartphone operation is achieved in general by replacing some functional blocks with new ones or the entire RA code with a new one.

4.2.2 Stakeholders

- End users: the users of the smartphones accessing internet and other similar mobile data services.
- Network operators:
  - operate and maintain the required infrastructure;
  - might provide information on the availability of new RAP(s) to the end users; might provide the new RAP(s) to the end users.
- Software Manufacturer: may provide new RAP(s) for optimizing the operation of smartphone.
- National Regulatory Authority: provides framework for certification of new RAP(s) provided by software manufacturers.

4.2.3 Information Flow

4.2.3.1 Information Flows for Scenario "Optimize the operation of Smartphone"



NOTE: The RAP(s) shown in Figure 4.2.3.1-1 is for functional block(s) of desired communication protocol(s) or entire RAT.

Figure 4.2.3.1-1: Information Flow for Scenario "Optimize the operation of Smartphone"

NOTE: The "required information" for the Regulation Administration is issued by a suitable source. In this Use Case, no assumption on the responsible party for regulatory compliance is made.

4.3 Use Case "Connected Vehicle Radio Reconfiguration"

4.3.0 General

Since the lifetime of automotive communication components is substantially longer (> 10 years) compared to smartphones (~2 years), it seems to be necessary for the communication platform in a vehicle to cope with the new communication standard through the SW reconfiguration. The challenge is to ensure that a radio communications component remains relevant over the entire life-time of a vehicle, i.e. 10 years and beyond. It is almost certain that a V2X framework feature-set will evolve within this period. SW Reconfiguration will enable Manufacturers to replace specific SW and thus maintain related feature-sets up-to-date without requiring changes to the hardware. Accordingly, the use case for the connected vehicle should be based on the SW reconfiguration of the communication platform in accordance to the changes in the communication standard being used in vehicular communications.

4.3.1 Scenario "Upgrade of Feature-Set"

It is expected that LTE C-V2X will further evolve towards 5G New Radio based V2X services and beyond. Consequently, new features will be added by a continued standardization activity. In this scenario, it is assumed that an initial radio component design will comprise supplementary computational and memory resources which may remain unused during a first phase; with upcoming new features, however, corresponding software components will be made available to provide required feature-sets by exploiting those resources. Typically, the resources include FPGA (Field Programmable Gate Array), DSPs (Digital Signal Processors), memory and other resources.

4.3.2 Scenario "Addressing Vulnerabilities"

Automotive communication components are a likely target for malicious attacks due to the large scale deployment, the high potential for causing damage through attacks and the long life-time of radio components. Indeed, the life-time corresponds to the life-time of a vehicle which is typically 10 years or more. It is therefore likely that vulnerabilities will be identified during this substantial time period. Those vulnerabilities may relate to design choices, protocol weaknesses, etc. When such a vulnerability is identified, it is essential to modify affected functionalities such that no damage can be caused to concerned vehicles and persons. Preferably, this modification is implemented on all relevant vehicles within the shortest time possible. Over-the-Air Software updates are a suitable means to achieve this objective.

4.3.3 Stakeholders

- End users: the users of the connected vehicles accessing internet and other similar mobile data services.
- Network operators:
  - operate and maintain the required infrastructure;
  - might provide information on the availability of new RAP(s) to the end users; might provide the new RAP(s) to the end users.
- Vehicle manufacturers: provide information on the availability of new RAP(s) to the network operators; might provide new RAP(s) to network operators.
- National Regulatory Authority: provides framework for certification of new RAP(s) provided by vehicle manufacturers.

4.3.4 Information Flow

4.3.4.1 Information Flows for Scenario "Upgrade of feature-Set" and "Addressing Vulnerabilities"

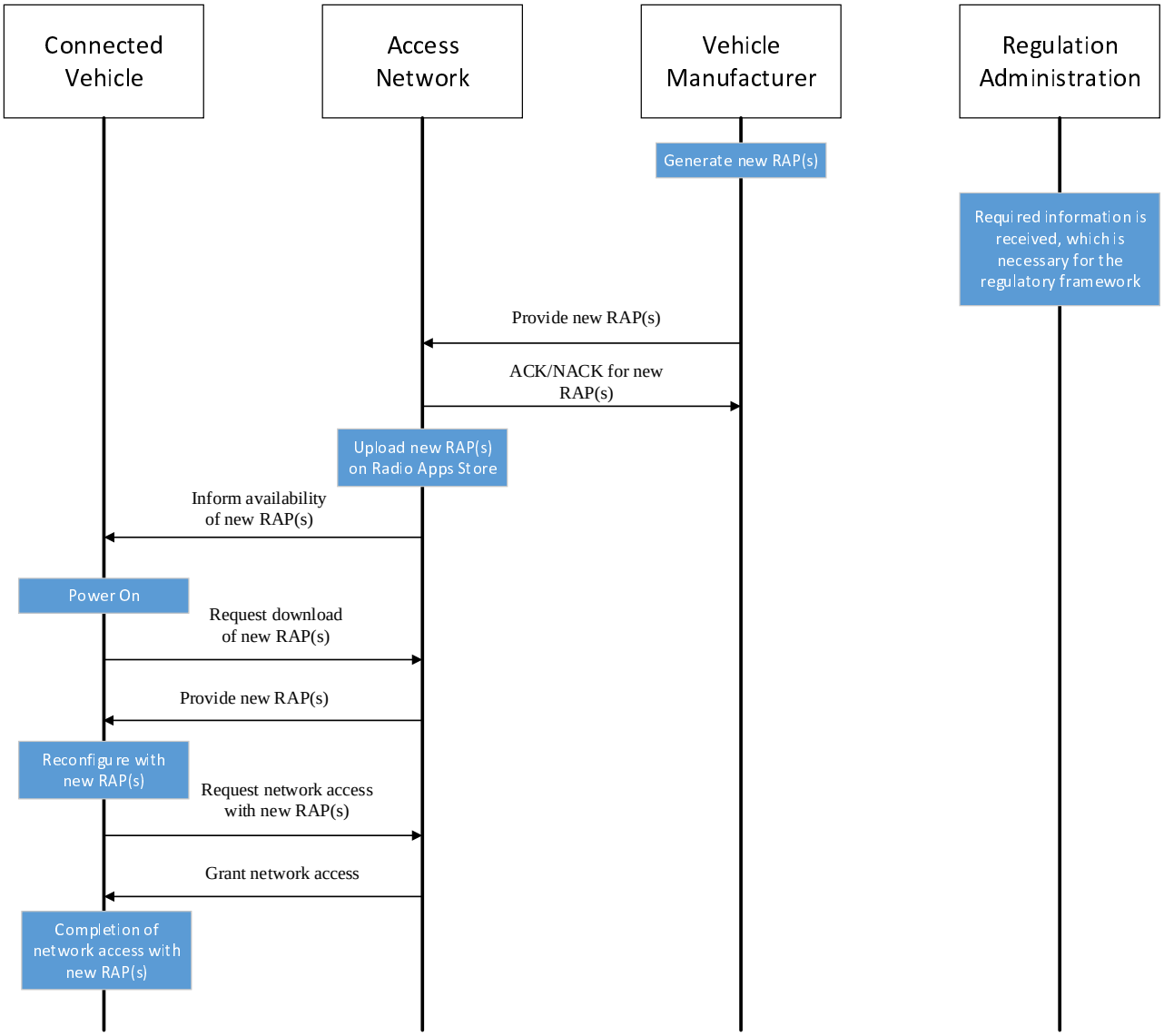


Figure 4.3.4.1-1: Information Flow for Scenarios "Upgrade of feature-Set" and "Addressing Vulnerabilities"

Note that the RAP(s) shown in Figure 4.3.4.1-1 is for upgrade of feature-set or addressing vulnerabilities. A typical example RAP for the upgrade of feature-set might be a 5G New Radio (NR) protocol that will be available as the standard of mobile communications evolves from 4G to 5G. A typical example for the addressing vulnerabilities might be a security-related RAP as a countermeasure against malicious attack(s). It is noteworthy that vehicle manufacturers not the 3rd party software manufacturer provide the RAP in the vehicle use case. The reason being so is that only the RAP of which the operation is fully verified is provided by vehicle manufacturers in the use case of connected vehicle.

NOTE: The "required information" for the Regulation Administration is issued by a suitable source. In this Use Case, no assumption on the responsible party for regulatory compliance is made.

4.4 Use Case "Network Radio Reconfiguration"

4.4.0 General

With the evolution of wireless standards, network functions need to be updated. In this Use Case, the installation of RadioApps is addressed in order to provide updated or new features which address the radio characteristics of the network. For example, a new Radio Access Technology may be made available through the installation of a software component. The installation of a single RAP may be sufficient if the target network functions are provided in a dedicated, single equipment such as a Small Cell owned by a User. In other cases, network functions are distributed across a variety of physical entities which all require dedicated software updates for the provisioning of a specific new service.

Typically, such equipment is then further connected to a larger network, for example through wireless or cabled backbone network access. In this Use Case, the User is able to alter or extend the functionalities of this equipment through installation of suitable RadioApps.

In other cases, network functions are distributed across a variety of physical entities. In this Use Case, the reconfiguration through RadioApps is possible through installation of Software Components in any equipment which requires functional changes in order to provide the new service.

4.4.1 Scenario "Single-Entity Network Radio Reconfiguration"

In this Scenario, a single radio entity is providing network/internet access to subscribers, for example a Small Cell owned by a User. Typically, such equipment is then further connected to a larger network, for example through wireless or cabled backbone network access. In this Scenario, the User is able to alter or extend the functionalities of this equipment through installation of suitable RadioApps. Software reconfiguration updates may be provided similar to the Smartphone Radio Reconfiguration context [i.1], [i.2], [i.3], [i.4], [i.5] and [i.6].

4.4.2 Scenario "Multiple-Entities Network Radio Reconfiguration"

In this Scenario, new features will typically not be limited to software reconfiguration of a single physical entity. Rather, Access/Core network functionalities may be distributed among multiple distinct physical entities, for example including a data centre and similar. A typical example is the deployment of a cellular network. Software reconfiguration thus typically requires the installation of software components on multiple physical entities.

4.4.3 Stakeholders

- End users: the users of the radio service.
- Network operators:
  - operate and maintain the required infrastructure;
  - might provide information on the availability of new RAP(s) to the end users; might provide the new RAP(s) to the end users.
- National Regulatory Authority: provides framework for certification of new RAP(s) provided by vehicle manufacturers.

4.4.4 Information Flow

4.4.4.1 Information Flows for Scenario "Single-Entity Network Radio Reconfiguration"

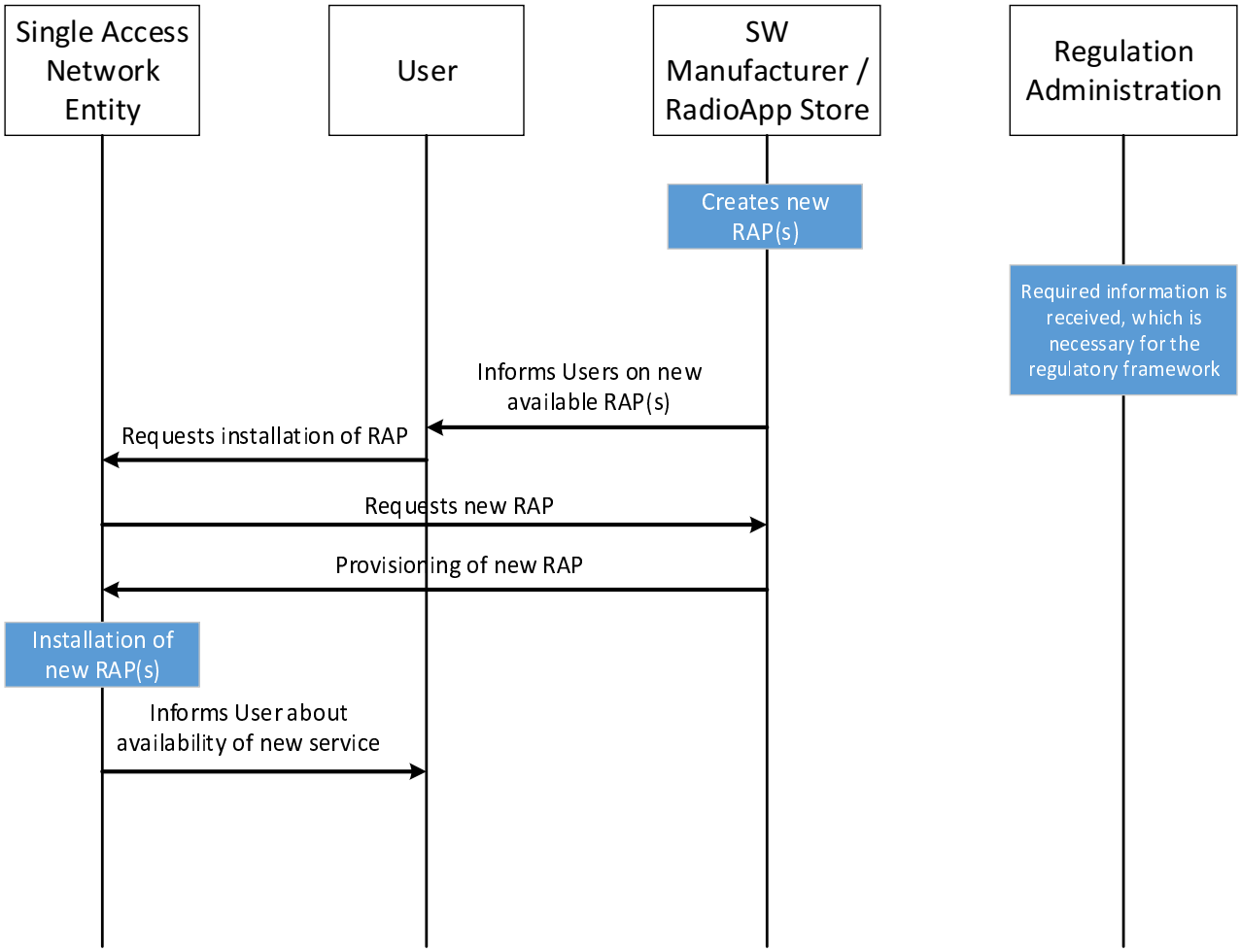


Figure 4.4.4.1-1: Information Flow for Scenario "Single-Entity Network Radio Reconfiguration"

In case of a single network access entity, the Software Reconfiguration framework is similar to the Mobile Device Software Reconfiguration framework [i.1], [i.2], [i.3], [i.4], [i.5] and [i.6].

NOTE: The "required information" for the Regulation Administration is issued by a suitable source. In this Use Case, no assumption on the responsible party for regulatory compliance is made.

4.4.4.2 Information Flows for Scenario "Multiple-Entities Network Radio Reconfiguration"

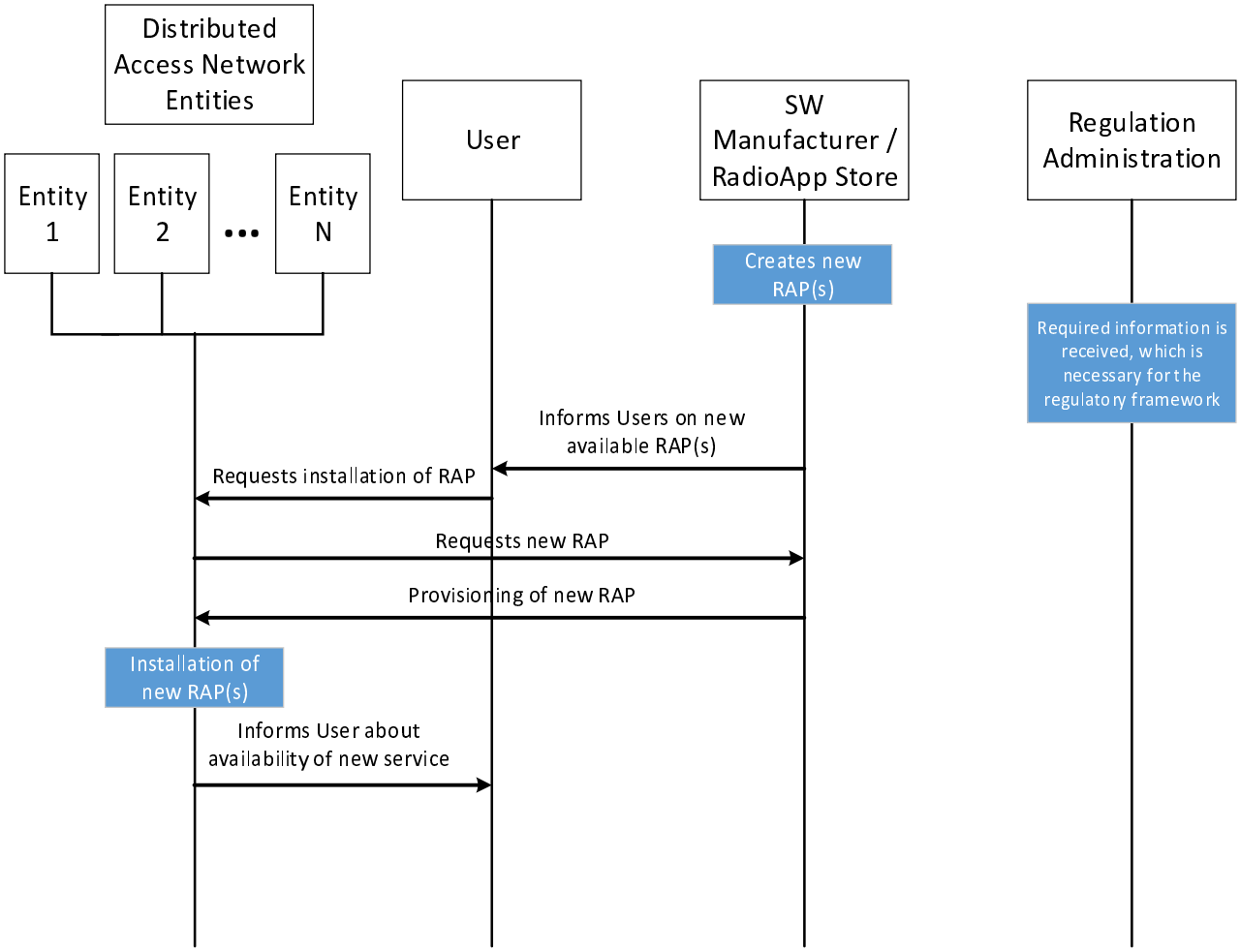


Figure 4.4.4.2-1: Information Flow for Scenario "Multiple-Entities Network Radio Reconfiguration"

In case of a distributed network access entities, the Software Reconfiguration framework needs to provide Software Components for all concerned entities.

NOTE: The "required information" for the Regulation Administration is issued by a suitable source. In this Use Case, no assumption on the responsible party for regulatory compliance is made.

4.5 Use Case "IoT Device Reconfiguration"

4.5.0 General

Future IoT devices, including 5G, will address a substantial variety of use cases, encompassing for example gaming, voice communication, medical applications, industrial automation, etc. Each of such vertical applications has its particular needs in terms of features, form factors, etc. Due to quasi-infinite possibilities, it is unlikely that chipmakers will offer tailored components for each of the vertical applications. Rather, a limited number of generic and reconfigurable components will be made available which are suitably tailored to the target market through SW components. The ETSI SW Reconfiguration solution provides a suitable ecosystem to support the future IoT market needs. Therefore, this clause considers use cases for optimizing the required communication services in a generic IoT communication platform through the SW reconfiguration by downloading the desired Radio Application code. Two categories of use cases are further considered: firstly, optimization by pre-provisioning of a Radio Application at manufacture time and, secondly, optimization by downloading of a Radio Application from the Radio Apps Store over-the-air. Indeed, some classes of IoT devices will be limited by various operational factors, such as the capabilities of the hardware platform, the allowed peak power consumption, or the available downlink bandwidth. Such devices will be restricted to pre-provisioning, while those with adequate resources will be able to update their Radio Applications over-the-air.

4.5.1 Scenario "Optimization by pre-provisioning of a RA at manufacture time"

In this scenario, the RA code is optimized during the "manufacture time" according to a required application through a pre-provisioning of the RA code for IoT devices which are pertaining to various restrictions in terms of hardware platform capabilities, allowed peak power, available downlink bandwidth, etc. Due to the various restrictions, the reconfiguration of the hardware platform after the "manufacture time" might be limited, for instance, to a modification of parameters for managing the radio characteristics, etc.

4.5.2 Scenario "Optimization by downloading of a RA from Radio Apps Store"

In this scenario, the RA code is optimized according to a required application through a software download of the RA code from RadioApp Store for IoT devices which are free from restrictions in terms of hardware platform capabilities, allowed peak power, available downlink bandwidth, etc. Since the hardware platform of this kind of IoT devices are reconfigurable, the IoT device can flexibly be reconfigured to Sensor, Access Point, Mobile phone, etc., upon the request of user.

4.5.3 Stakeholders

- End users: the users of the IoT Devices accessing internet and other similar mobile data services.
- Network operators:
  - operate and maintain the required infrastructure;
  - might provide information on the availability of new RAP(s) to the end users; might provide the new RAP(s) to the end users.
- Software Manufacturer: may provide new RAPs for optimizing the operation of IoT Devices.
- National Regulatory Authority: provides framework for certification of new RAP(s) provided by software manufacturers.

4.5.4 Information Flow

4.5.4.1 Information Flows for Scenario "Optimization by pre-provisioning of a RA at manufacture time"

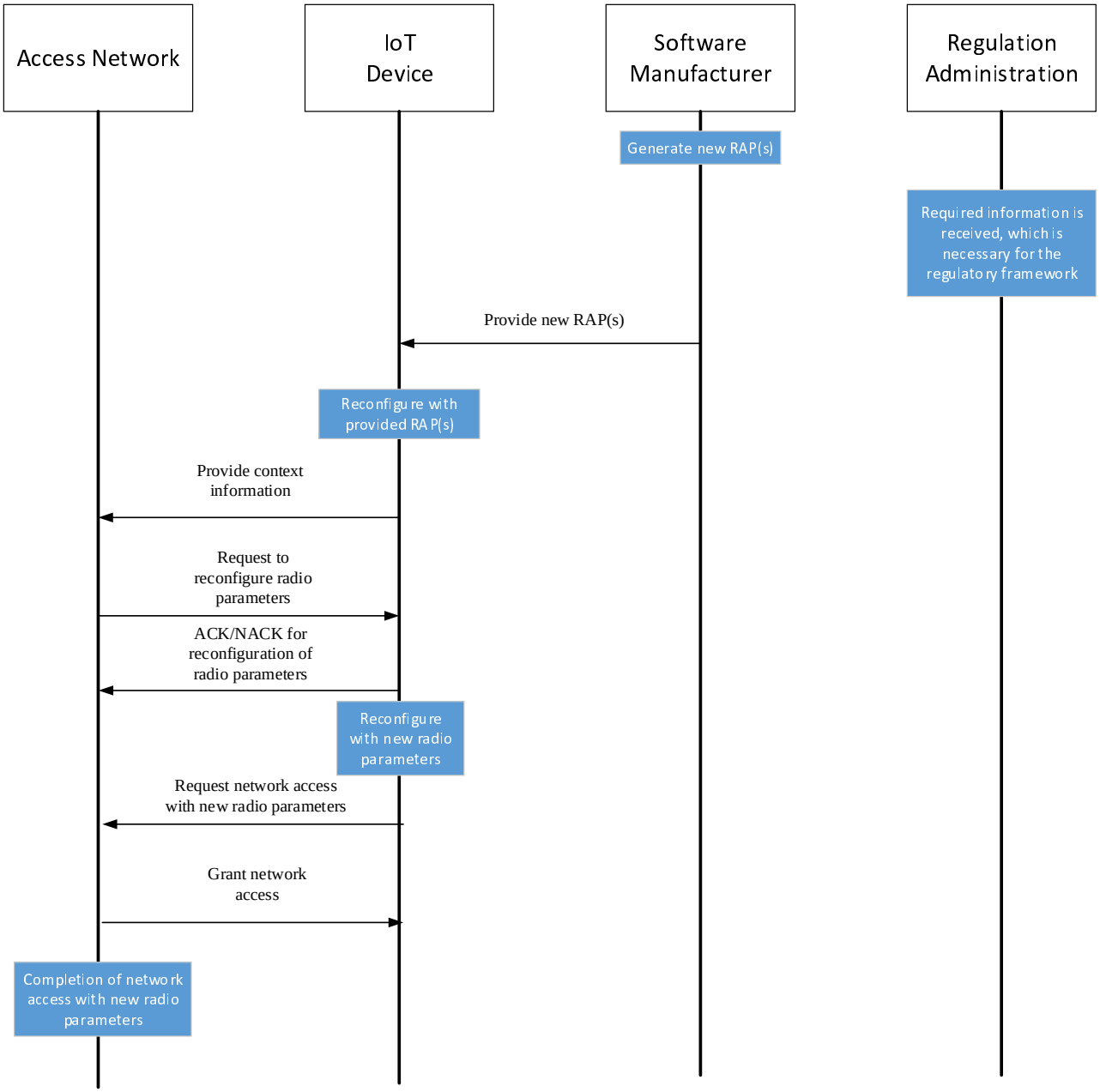


Figure 4.5.4.1-1: Information Flow for Scenario "Optimization by pre-provisioning of a RA at manufacture time"

Note that it is the "manufacture time" of an IoT device until the present RAP(s) is reconfigured with provided RAP(s). The RAP specifies a specific application assigned to the IoT device which operates with a reconfigurable hardware platform.

NOTE: The "required information" for the Regulation Administration is issued by a suitable source. In this Use Case, no assumption on the responsible party for regulatory compliance is made.

4.5.4.2 Information Flows for Scenario "Optimization by downloading of a RA from Radio Apps Store"

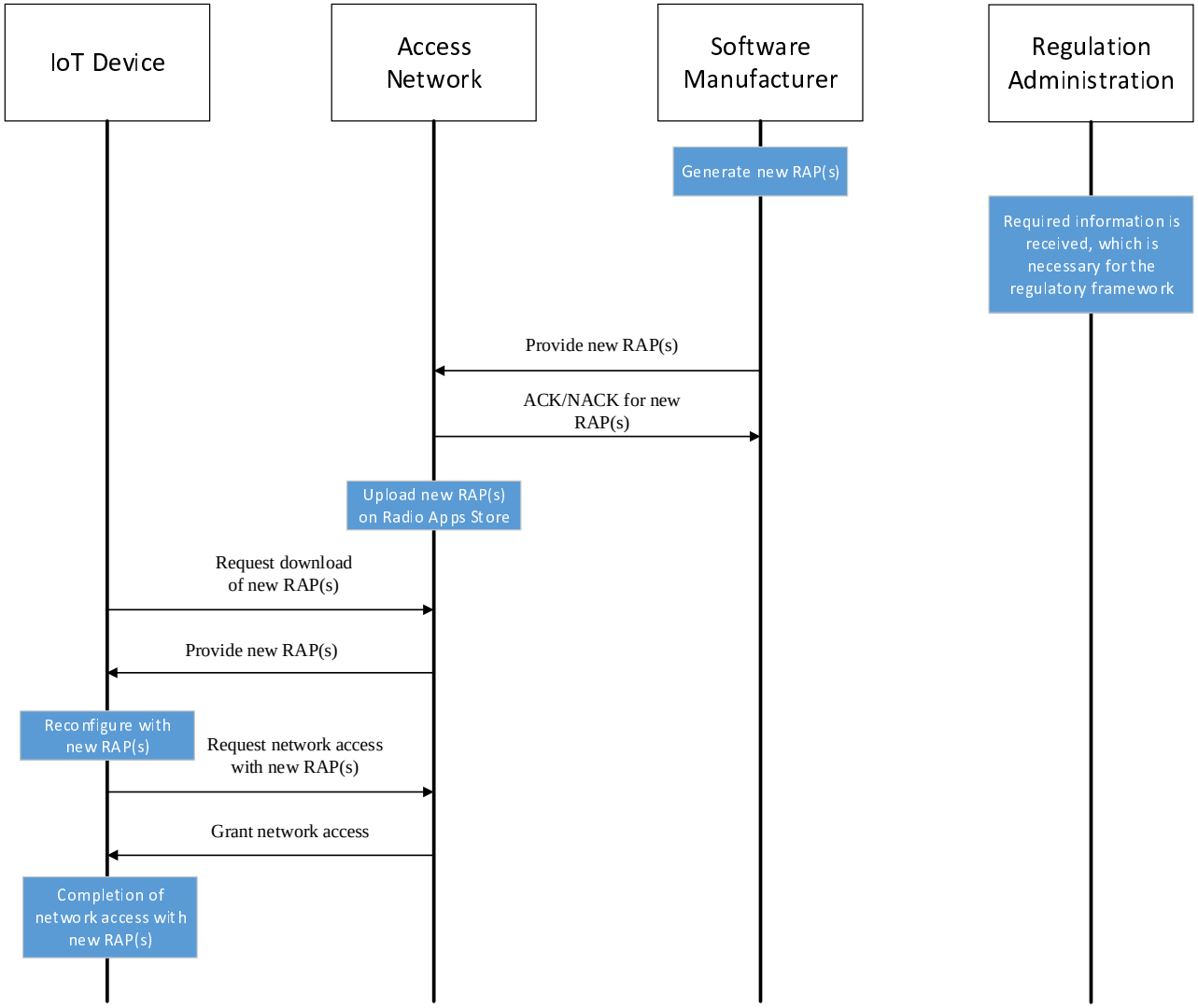


Figure 4.5.4.2-1: Information Flow for Scenario "Optimization by downloading of a RA from Radio Apps Store"

Note that the reconfiguration was possible only for the "manufacture time" in the case of "Optimization by pre-provisioning of a RA at manufacture time", while the reconfiguration is allowed any time in the case of "Optimization by downloading of a RA from Radio Apps Store" because there is no restriction on this kind of IoT devices in terms of hardware platform capability, allowed peak power, available downlink bandwidth, etc.

NOTE: The "required information" for the Regulation Administration is issued by a suitable source. In this Use Case, no assumption on the responsible party for regulatory compliance is made.

4.6 Use Case "Radio Reconfiguration through an external Component"

4.6.0 General

While radio connectivity in the Consumer Electronics market is mostly provided by device integrated components, there also exist radio external components that can be plugged on host devices, and thus form composite devices. Such external components can take the form of e.g. USB sticks, PCI-e daughter cards, etc. The ETSI SW Reconfiguration solution provides the tools necessary to securely manage Radio Applications and ensure regulatory compliance.

4.6.1 Scenario "Standalone external components"

The scenario concerns standalone radio external components that embed all the capabilities necessary to radio processing. The host device is not involved in radio processing but may configure operational parameters as allowed by the external component (which may implement the ETSI SW Reconfiguration Architecture). Thus, the separation between the host device and the external component is clear and embodied by the physical interface between the two. On the host device, only a device driver is necessary to operate the external component and integrate it into the networking stack - which may be done through the Multiradio Interface (MURI). In order to reconfigure the external component, the host device may be used as a staging area to store Radio Applications which are then loaded on the external component via the device driver (e.g. the device driver may leverage the Administrator). In this case, however, the decision to accept and instantiate the Radio Application remains with the external component. Alternatively, reconfiguration may be handled by the external component itself such that the host device is not involved at all.

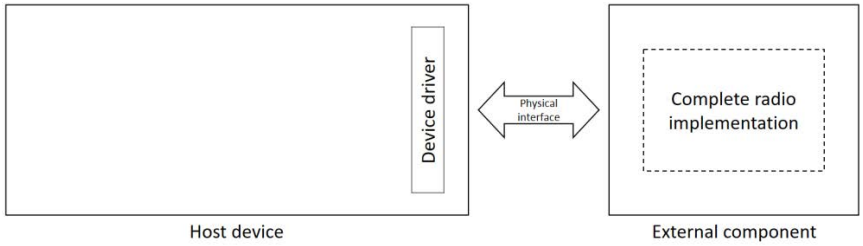


Figure 4.6.1-1: simplified view of host and external component interaction with a standalone external component

4.6.2 Scenario "Host dependent external component"

This scenario addresses external components that depend on the host device to perform radio processing. In this case, the software necessary to implement a given Radio Access Technology is loaded on the host device, with the external component only providing specific capabilities (e.g. converters, radio front-end, etc.). Thus, a virtual device is created on the host device: it binds together the external component and software components of the Radio Application that are instantiated on the host device. The separation between the host device and the external component is embodied by a logical interface on the host device. The host device may implement most of the components of the ETSI SW Reconfiguration Architecture. The decision to install Radio Applications, and how to instantiate them, rests with the host device.

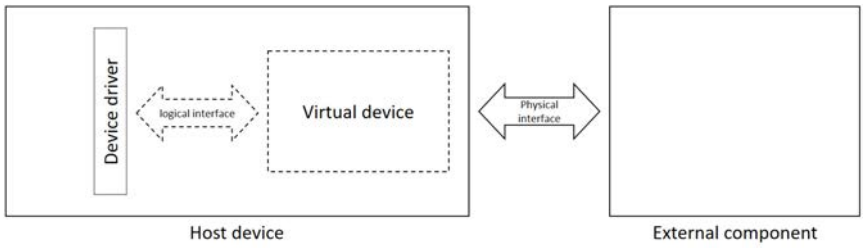


Figure 4.6.2-1: simplified view of interactions with the host dependent external component

4.6.3 Stakeholders

The following stakeholders are defined for the scenario "Standalone external components":

- End users: the users of the host device combined with an external component, accessing internet and other similar mobile data services.
- External Component Manufacturer: provides RAPs for the External Component, manages RAPs on a Radio App Store, may provide Device Driver for host devices.
- National Regulatory Authority: provides framework for certification of new RAPs provided by External Component Manufacturer.

The following additional stakeholders are defined for the scenario "Host dependent external component":

- Host Device Manufacturer: manufactures the host device and provisions it with an Operating System and other software components, possibly with an execution environment suitable for Radio Applications.
- Software Manufacturer: develops Radio Applications.
- Manufacturer: composition of the External Component Manufacturer, the Host Device Manufacturer, and the Software Provider for the purpose of regulatory compliance.

4.6.4 Information Flows

4.6.4.1 Information Flows for Scenario "Standalone external components"

NOTE 1: Figure 4.6.4.2-1 is applicable to full and/or partial radio processing in the host device. Figure 4.6.4.1-1 and Figure 4.6.4.1-2 are applicable to full radio processing in the external device.

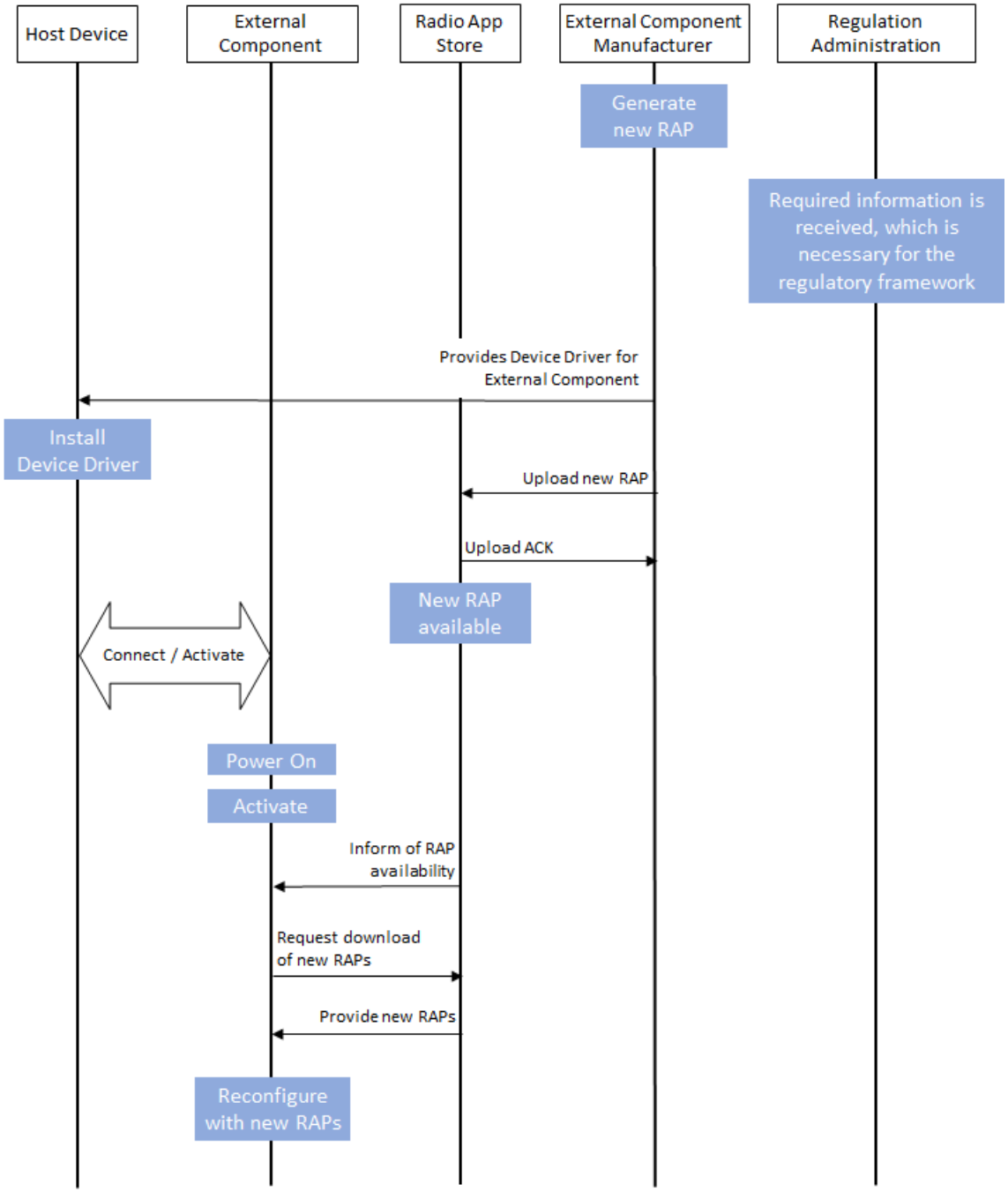


Figure 4.6.4.1-1: Information Flow for Scenario "Reconfiguration of a standalone external component when the installation is handled by the external component"

NOTE 2: The "required information" for the Regulation Administration is issued by a suitable source. In this Use Case, no assumption on the responsible party for regulatory compliance is made.

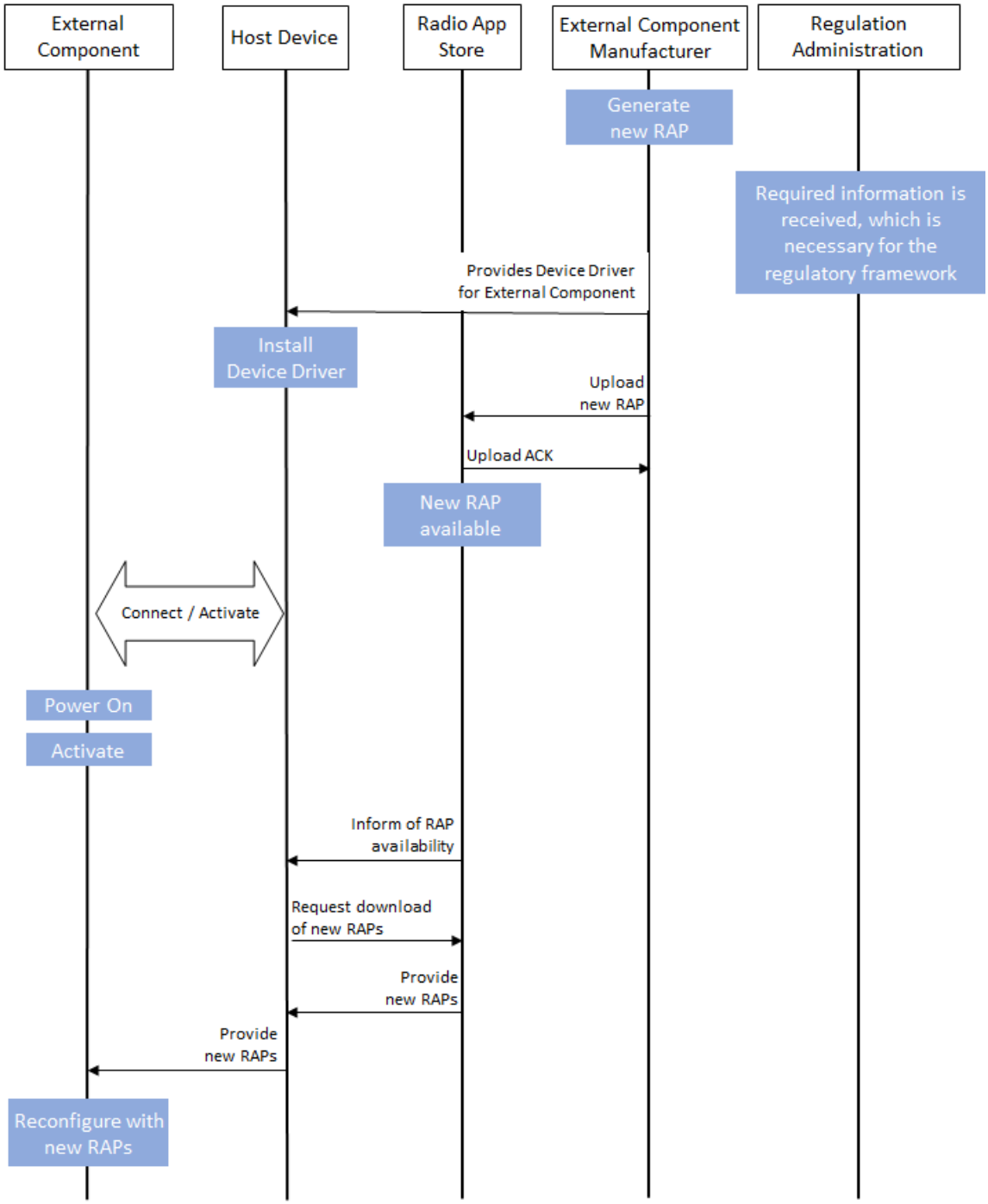


Figure 4.6.4.1-2: Information Flow for Scenario "Reconfiguration of a standalone external component when the installation is handled by the host device"

NOTE 3: The "required information" for the Regulation Administration is issued by a suitable source. In this Use Case, no assumption on the responsible party for regulatory compliance is made.

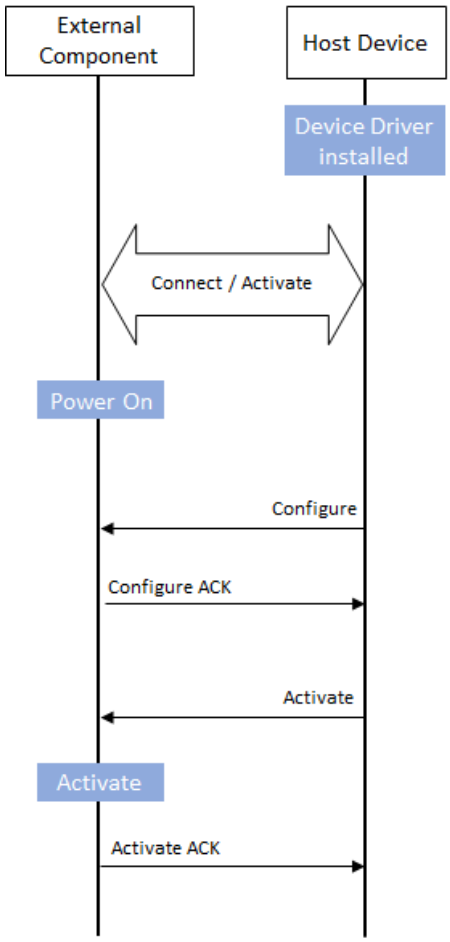


Figure 4.6.4.1-3: Information Flow for Scenario "Activation procedure of a standalone external component"

4.6.4.2 Information Flows for Scenario "Host dependent external component"

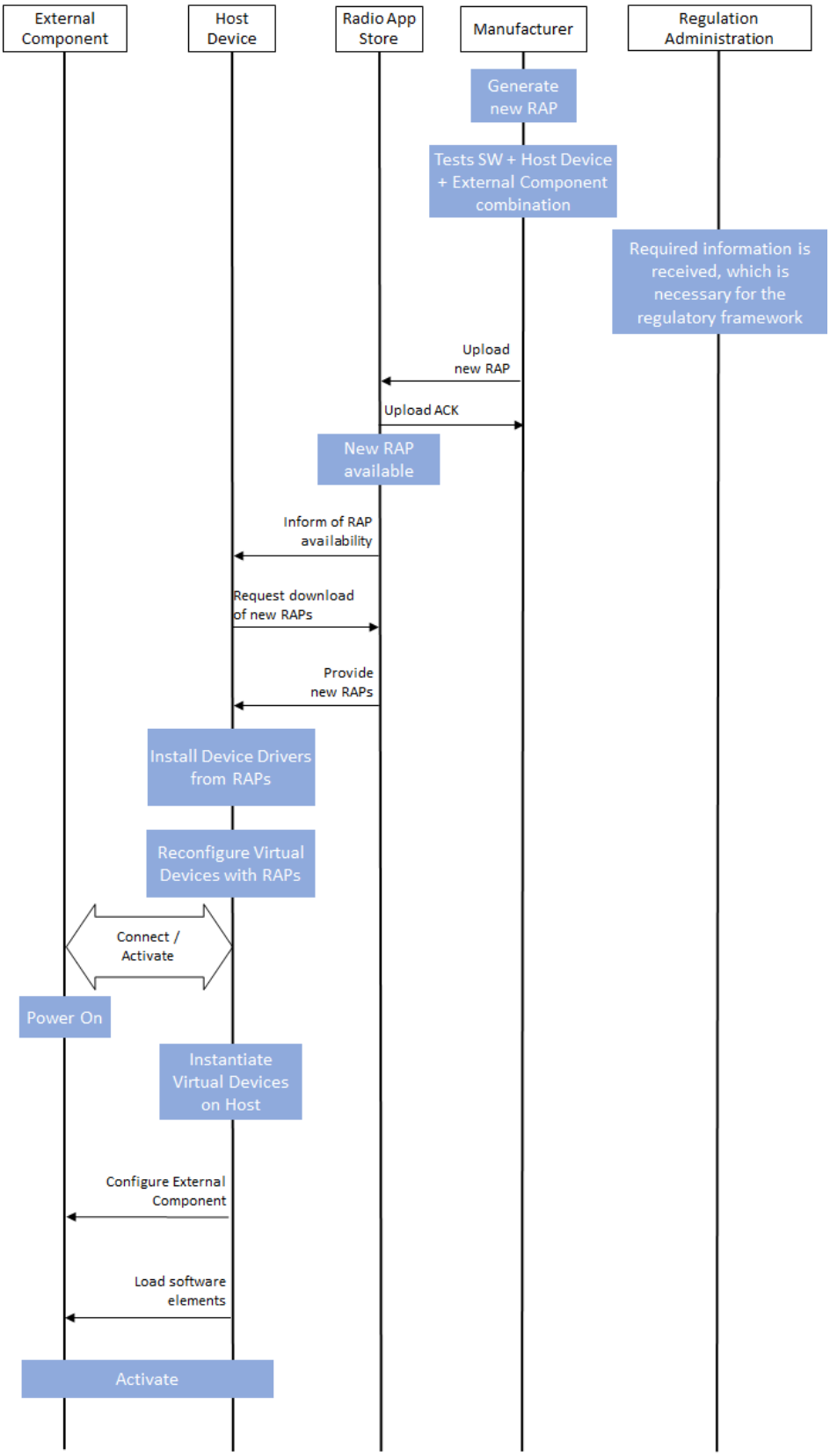


Figure 4.6.4.2-1: Information Flow for Scenario "Reconfiguration and activation of a host dependent external component"

NOTE: The "required information" for the Regulation Administration is issued by a suitable source. In this Use Case, no assumption on the responsible party for regulatory compliance is made.

4.7 Use Case "Reconfigurable Satellite Telecom Payload"

4.7.1 Introduction

Evolution of satellite communication systems towards providing more complex telecommunication services requires steady efforts in development of the onboard system architecture. The complexity demand is driven by requirements to support different frequency bands and radio transmission power, complexity of antenna coverage, onboard processing functions and their flexibility. Lifetime of satellites varies from a few years for Low Earth Orbiting (LEO) satellites until 10 or even 15 years for GEO (*Geostationary* Earth Orbit) satellites. This fact and the rapid progress in the field of digital communications raise the problem of technological obsolescence of onboard telecom payload. The emergence of new signal processing algorithms and new standards that provide reliable and high-speed transmission of information requires the reconfiguration of the onboard equipment.

Satellite communication systems are considered as a part of the global network infrastructure with the integrated satellite segment. Therefore, they should be provisioned within the same management framework as the terrestrial segment. Management solutions accepted in 5G networks is based on the SDN/NFV concept [i.10], [i.11] assuming virtualization of network functions and automatic network provisioning. This is another driver for the on-board telecom equipment reconfigurability.

The current standardized satellite communication systems architecture [i.8] supposes two types of network topology presented in Figure 2 of [i.8].

- A star network topology is defined by the star arrangement of links between the hub station (or Internet access point) and multiple remote stations. A remote station can only establish a direct link with the hub station and cannot establish a direct link to another remote station.
- A mesh network is defined by the mesh arrangement of links between the stations, where any station can link directly to any other station. The star topology can be considered as one special case of the mesh topology. In case of LEO satellites, a quite big satellite constellation including hundreds or even thousands satellites is considered instead of one satellite. Multiple inter-satellite links shown in Figure 4.7.1-1 appear in mesh structure in this case and satellites play role of routers or switches.

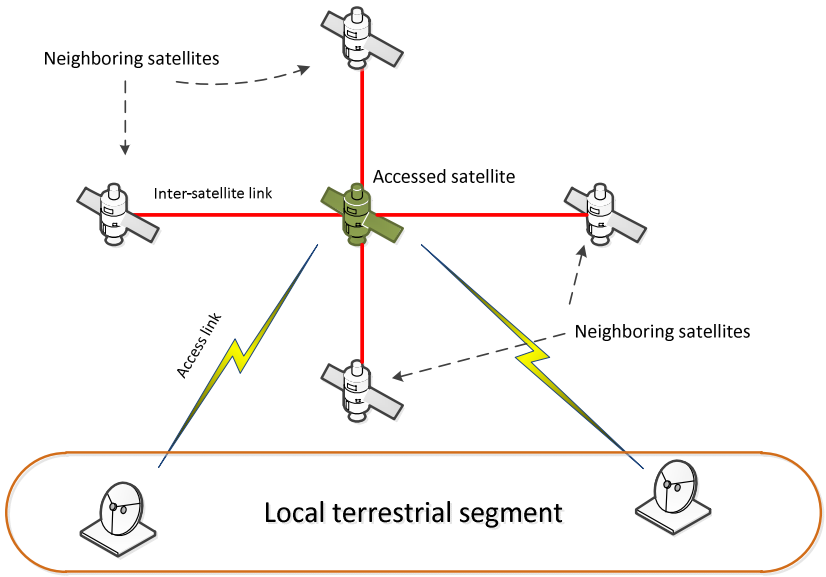


Figure 4.7.1-1: LEO Constellation.

An onboard telecom payload may use either a non-regenerative or a regenerative architecture [i.8]:

- A non-regenerative architecture refers to a single architecture, commonly called a "bent-pipe architecture". This architecture does not terminate any layers of the air interface protocol stack in the satellite - the satellite simply transfers the signals from the user links to the feeder links transparently.
- A regenerative architecture is the range of other architectures that provide additional functionality in the satellite. In these architectures, the satellite functions terminate one or more layers of the air interface protocol stack in the satellite.

The bent-pipe architecture is illustrated in Figure 3 of [i.9]. It works for the star topology. The following components of this architecture are subject for reconfiguration:

- RF transceiver: carriers, power levels, bandwidths.
- Switches.
- Beam formers (Tx and RX).
- Input and output MUXs.

The regenerative architecture is illustrated in Figure 4 of [i.9]. It is applied in case of the mesh topology. The regenerative part consists of modem L1/L2 components. The simplified version includes the header-only on-board demodulator/modulator to route packets without regeneration for higher throughput and waveform flexibility. Additionally to the previous case, modem components implemented in software are subject for reconfiguration e.g.:

- Modulator.
- Demodulator.
- Encoder.
- Decoder and etc.

4.7.2 Scenario "Access Links Provisioning"

For the mesh topology, a satellite is connected to user satellite terminals via user access links or for the start topology, the satellite is connected to a hub via the feeder access link and to user satellite terminals via user access links. In the scenario telecom payload parameters related to the RF parts (Rx and Tx), beam formers (Rx and Tx) and switches are the subject for reconfiguration. The information flow for this scenario is shown in Figure 4.7.5.1-1. The Satellite Control Center (SCC) is a managing object initiating parameters provisioning. SCC moves a satellite board to the provisioning state by sending "provisioning request". If this movement is correct than the satellite send "ack" to confirm readiness for receiving provisioning parameters. SCC sends provisioning parameters used for parametrical reconfiguration of e.g. the bent-pipe architecture. The Regulation Administration should approve these actions prior their execution.

4.7.3 Scenario "Regenerator Reconfiguration"

In this scenario, SCC replaces obsolete or incorrect software components of the regenerative part of the satellite telecom payload or install a new Radio Application on the board. Information flow related to this scenario is shown in Figure 4.7.5.2-1. SCC sends "new RAP request" to the Radio Application Store to request a RAP with new software components to update an onboard Radio Application or with a new Radio Application to install it on the satellite board. After receiving the new RAP from the Radio Application Store SCC initiates the new RAP onboard installation by sending a request "install new RAP" to the satellite. This request includes the RAP and activate reconfiguration procedure after the RAP downloading. As result of the reconfiguration onboard procedure, the new RAP is installed and activated on the board. All these actions should be approved by the Regulator Administration. For this purpose, all needed information should be sent to the Regulation Administrator prior onboard reconfiguration.

4.7.4 Stakeholders

The following stakeholders are defined:

- End users: the users of Terminal Equipment for Satellite Communication (which may be reconfigurable also).
- National Regulatory Authority: Entity providing framework for certification of new RAPs to Satellite Telecommunication Payload.
- Manufacturer: Manufacturer of the Satellite Telecommunication Payload and/or RAP.
- Satellite Operators: Entity installing new RAPs to Satellite Telecommunication Payload, e.g. in order to upgrade functionalities, etc.

4.7.5 Information Flows

4.7.5.1 Information Flows for Scenario "Access Links Provisioning"

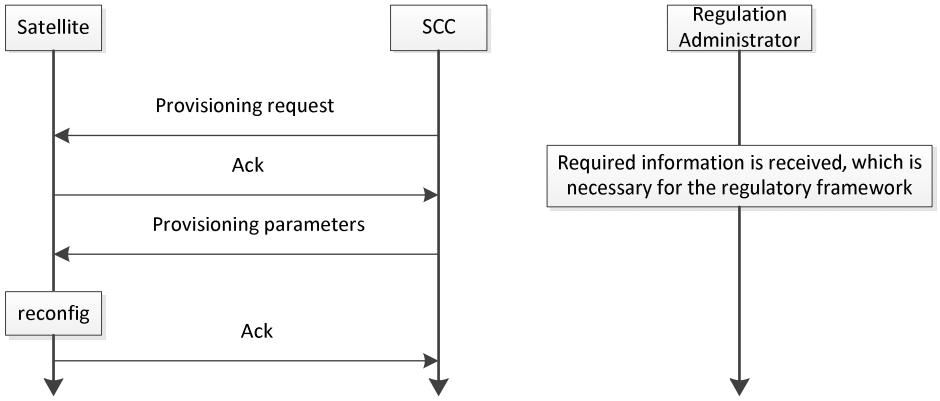


Figure 4.7.5.1-1: Information Flow for Scenario "Access Links Provisioning"

4.7.5.2 Information Flows for Scenario "Regenerator Reconfiguration"

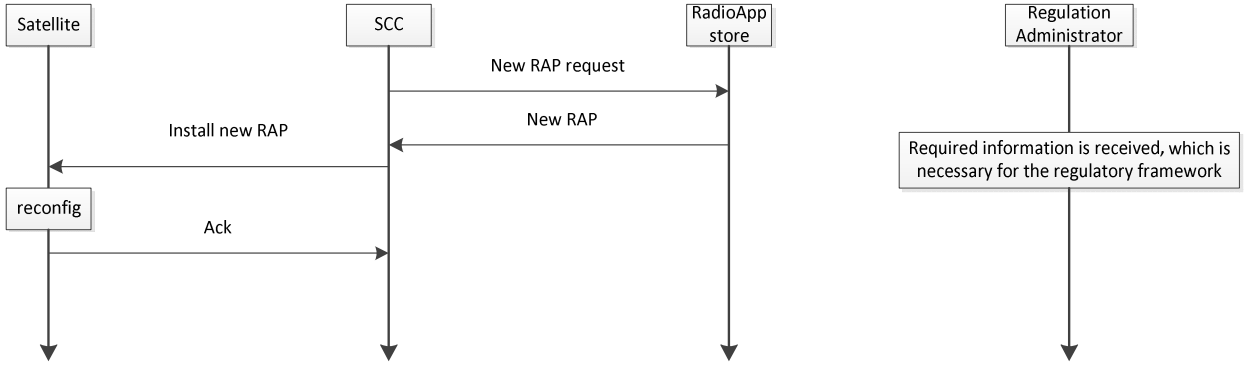


Figure 4.7.5.2-1: Information Flow for Scenario "Regenerator Reconfiguration"

4.8 Use Case "Bug-fix and security updates"

4.8.1 Introduction

Bug-fixes and security updates are essential to the maintenance of the Radio Application throughout its lifecycle. Bug-fixes help ensure that Radio Applications will behave according to specification even after the Radio Application has been installed on a device. For example, when Radio Applications are subject to automated testing the addition of new tests may uncover new, unwanted behaviour resulting from a design flaw. Operations in the field may place the equipment in an unexpected situation that is not properly handled by the Radio Application. For example, the introduction of a new Radio Access Technology may cause coexistence problems. A bug could have an adverse effect on radio processing, compliance to the essential requirements and objectives of the Radio Equipment Directive and other regulatory frameworks, as well as on higher protocol layers such as the RLC and the LLC, depending on the scope of the Radio Application Package.

Security updates help ensure the integrity of an implementation, in particular that a specially crafted input will not trigger a bug that could be exploited and compromise the implementation. Application security is an evolving field and implementations believed to be secure at some point in time may later become insecure as new attack methods are devised. Notwithstanding any other consideration, a rule of thumb is that the older the implementation, the higher the risk of finding security vulnerabilities. The compromise of a Radio Application may lead to a malfunction in the radio stack and in other device components, with effects equivalent to that of a bug. Such situation is to be avoided, in particular in systems with a high expectation of safety, where security support essential safety function. The net result being that a security vulnerability may void any assumption on the behaviour of an implementation, obtained e.g. from a testing framework or a certification mechanism.

It is therefore critical that Radio Applications can be updated in order to address bugs and security vulnerabilities. This is supported by the ETSI SW Reconfiguration solution where new versions of Radio Applications can be distributed to devices - either via the RadioApp Store or in an out-of-band fashion.

The "Bug-fix and security updates" use case is relevant to all other use cases in the present document, especially to the use case "Connected Vehicle Radio Reconfiguration".

4.8.2 Scenario "Automated Updates"

In this scenario the radio device detects the availability of a new Radio Application Package via the capabilities provided by the ETSI SW Reconfiguration solution, downloads it, verifies it, and installs it in an autonomous fashion. While the procedure is completely automated, in some cases the end-user may be slightly involved in order to provide consent, for example to agree to automated updates or temporarily disable them, or to agree to the installation of a Radio Application at the time it is ready to be installed on the device.

4.8.3 Scenario "Manual Updates"

In this scenario updates are provided to end-users for them to install manually, due to constraints that do not allow automated updates. For example, the radio device may not have access to a RadioApp Store due to limited connectivity, or the end-user should take precautions, such a field testing, before deploying the Radio Application. Typically, the Radio Application Package is available on the RadioApp Store or a download area on the Internet, for the end-user to retrieve, or delivered via postal mail. The radio device provides an interface for the end-user to upload and install the Radio Application Package as part of their update procedure.

4.8.4 Stakeholders

The following stakeholders are defined:

- End users: the users of the equipment that supports the ETSI SW Reconfiguration solution.
- National Regulatory Authority: provides framework for certification of new RAPs provided by the radio device manufacturer.
- Manufacturer: composition of the Device Manufacturer, and the Software Provider for the purpose of regulatory compliance. The Manufacturer discovers (or is being notified of) a bug or a security vulnerability in a Radio Application.

4.8.5 Information Flows

4.8.5.1 Information Flows for Scenario "Automated Updates"

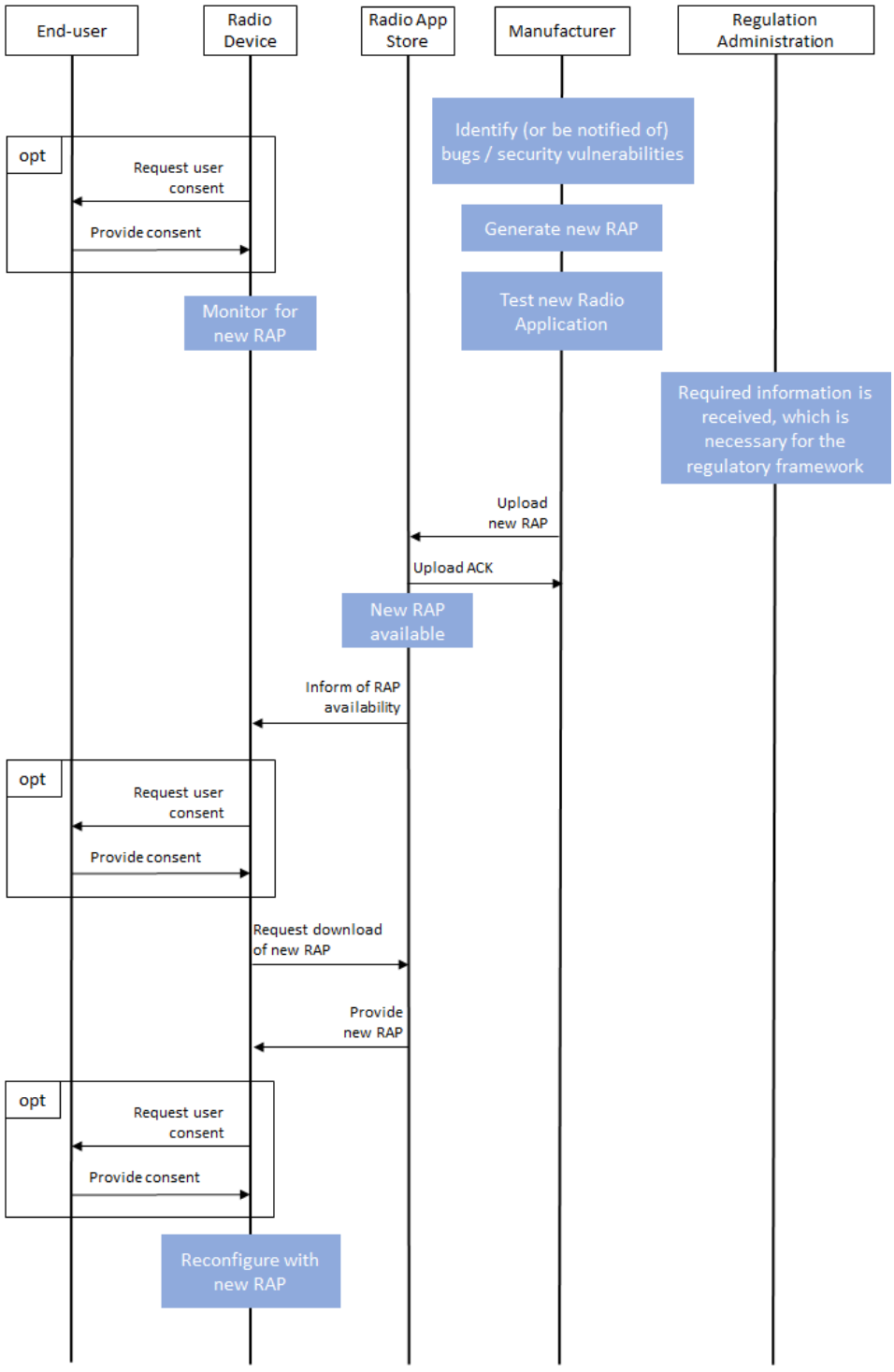


Figure 4.8.5.1-1: Information Flow for Scenario "Automated update of a Radio Application"

NOTE: The "required information" for the Regulation Administration is issued by a suitable source. In this Use Case, no assumption on the responsible party for regulatory compliance is made.

4.8.5.2 Information Flows for Scenario "Manual Updates"

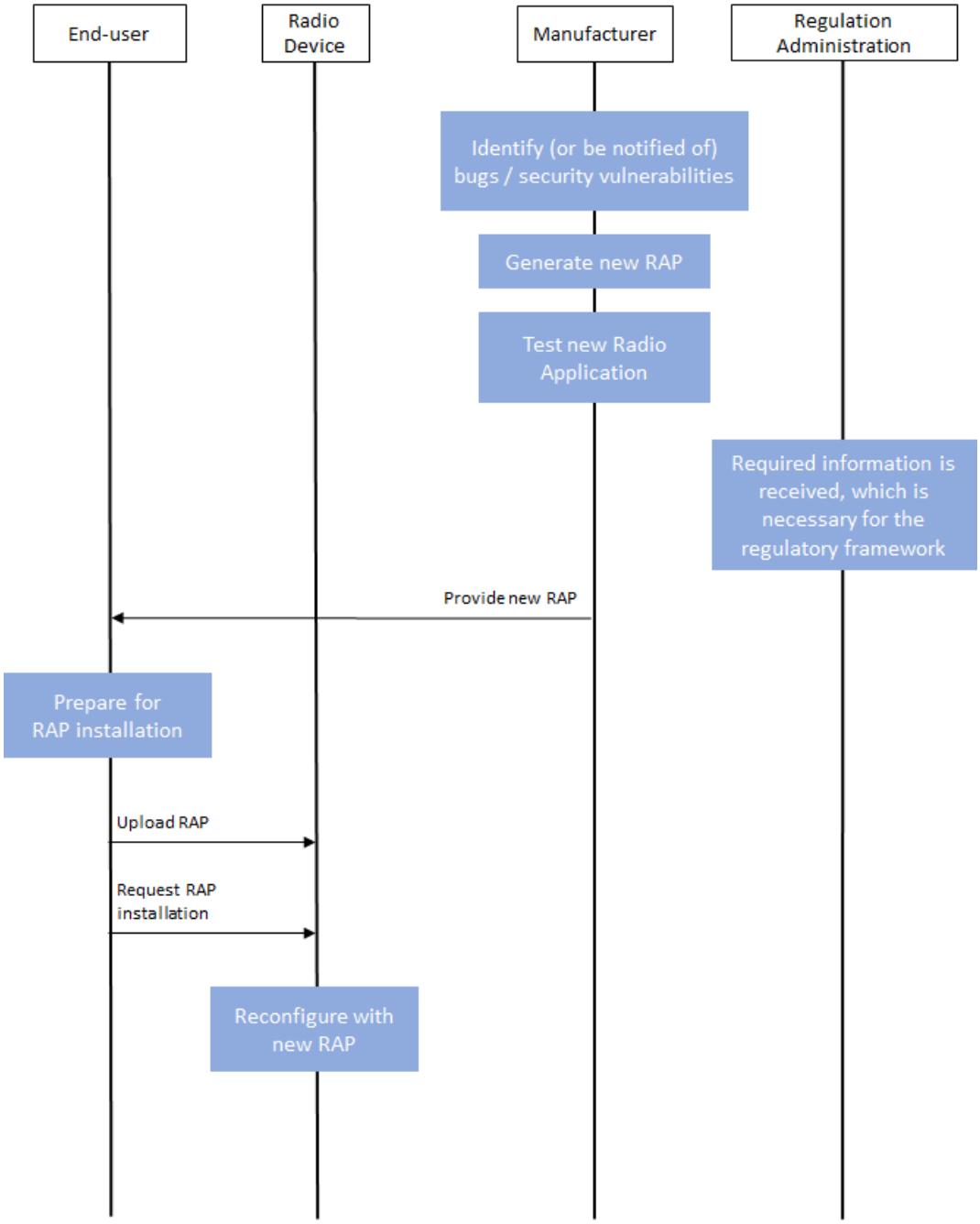


Figure 4.8.5.2-1: Information Flow for Scenario "Manual update of a Radio Application"

NOTE: The "required information" for the Regulation Administration is issued by a suitable source. In this Use Case, no assumption on the responsible party for regulatory compliance is made.

4.9 Use Case "Medical Applications"

4.9.1 Introduction

Medical applications, such as remote surgery, monitoring of patient's life support data, etc. requires highly reliable and stable communication systems. Still, software reconfiguration is expected to be broadly applied in order to enable users to have access to latest software updates and best possible functionalities. For example, in this context it is of specific importance to immediately correct any incorrect behaviour or security vulnerabilities and the like in order to ensure a maximum level of protection.

In case of medical applications, it is expected that a specific critical application will be executed on a reserved Radio Computer - instead of sharing a Radio Computer among multiple application as it may be done in the case of the Mobile Device Software Reconfiguration approach [i.1] to [i.6]. Thanks to this approach, all available computational resources will always be available to the concerned medical application - even in the most extreme and unlikely configuration cases. This way of operating is expected to provide the highest level of confidence to the users.

4.9.2 Scenario "Automated Updates"

In this scenario the radio device detects the availability of a new Radio Application Package via the capabilities provided by the ETSI SW Reconfiguration solution, downloads it, verifies it, and installs it in an autonomous fashion. While the procedure is completely automated, in some cases the end-user may be slightly involved in order to provide consent, for example to agree to automated updates or temporarily disable them, or to agree to the installation of a Radio Application at the time it is ready to be installed on the device.

4.9.3 Stakeholders

The following stakeholders are defined:

- End users: the users of the equipment that supports the ETSI SW Reconfiguration solution.
- National Regulatory Authority: provides framework for certification of new RAPs provided by the radio device manufacturer.
- Manufacturer: composition of the Device Manufacturer, and the Software Provider for the purpose of regulatory compliance. The Manufacturer discovers (or is being notified of) a bug or a security vulnerability in a Radio Application.

4.9.4 Information Flows

4.9.4.1 Information Flows for Scenario "Automated Updates"

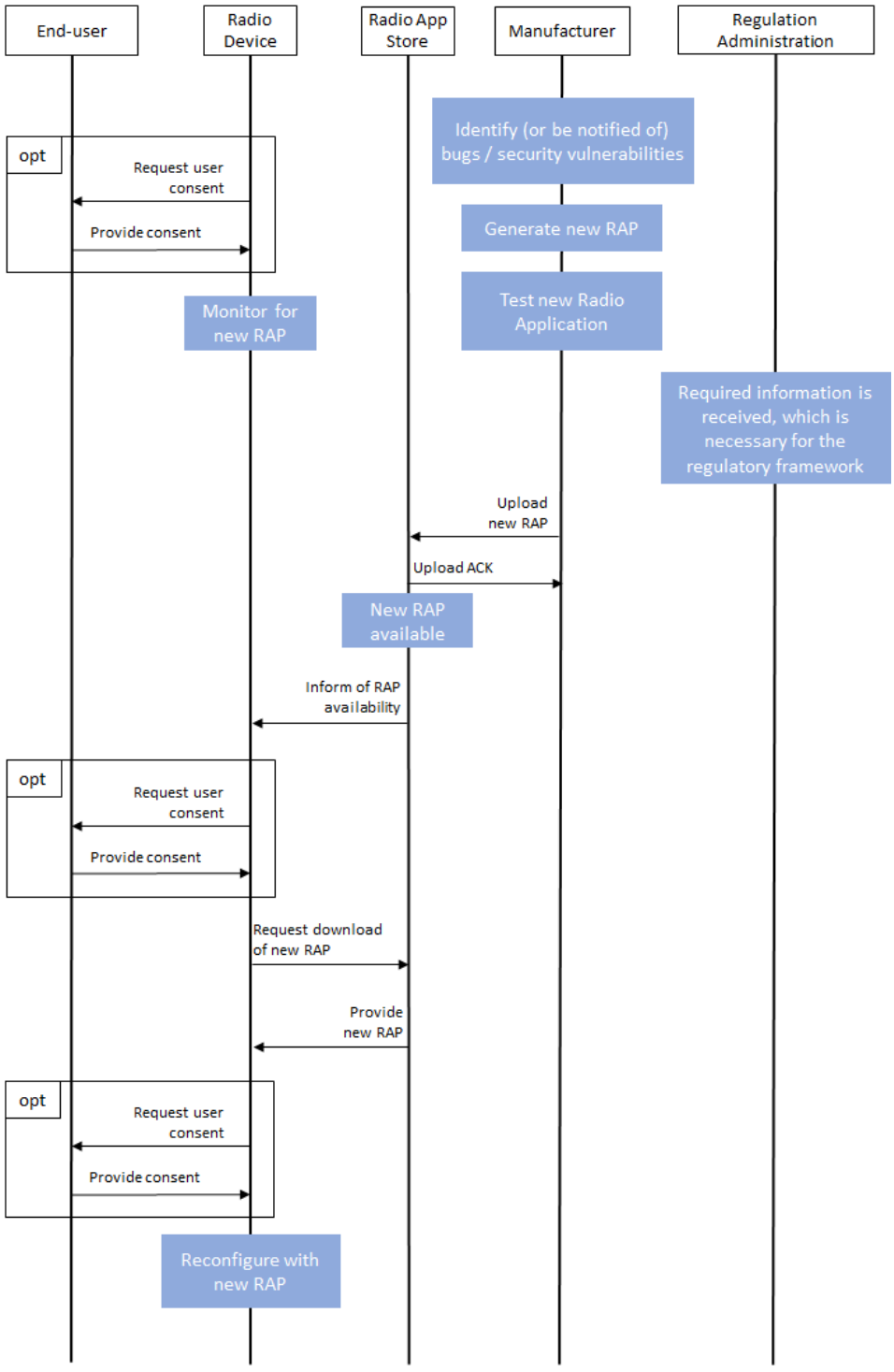


Figure 4.9.4.1-1: Information Flow for Scenario "Automated update of a Radio Application"

NOTE: The "required information" for the Regulation Administration is issued by a suitable source. In this Use Case, no assumption on the responsible party for regulatory compliance is made.

History

Document history		
V1.1.1	February 2018	Publication
V1.2.1	November 2019	Publication