ETSI TR 102 967 V1.1.1 (2014-03)

Reconfigurable Radio Systems (RRS);
Use Cases for dynamic equipment reconfiguration

Reference
DTR/RRS-03009

Keywords
conformance, radio, 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

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://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.

Foreword

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

1 Scope

The present document outlines the Use Cases which are related to the introduction of mechanisms to enable, for reconfigurable radio systems, the dynamic reconfiguration of equipment and its continuing conformity with the applicable legislation**.**

These Use Cases involve the dynamic reconfiguration of reconfigurable radio equipment after its initial certification and deployment. Such post-deployment reconfiguration will ensure the continued conformity in the new configuration to the applicable legislation. In some Use Cases, new mechanisms that enable reconfigurable devices to have their declaration of conformity dynamically verified may be introduced.

The present document also addresses the outcome of previous work such as that carried out in Europe by the Telecommunications Conformity Assessment and Market Surveillance Committee (TCAM) as a result of the Report drafted by its ad-hoc group on Software Defined Radio.

While the Use Cases presented in the present document are designed to support the novel radio reconfiguration features of the R&TTE Directive [i.2] that is applicable in Europe, the principles and the Use Cases outlined here are not limited to Europe and may also be appropriate for other regions.

2 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.

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 necessary for the application of the present document.

Not applicable.

2.2 Informative references

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] Report Recommendation ITU-R SM.2152: "Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS"), 2009.

[i.2] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

3 Definitions and abbreviations

3.1 Definitions

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

Cognitive Radio System (CRS): Radio system employing technology that allows the system: to obtain knowledge of its operational and geographical environment, established policies and its internal state; to dynamically and autonomously adjust its operational parameters and protocols according to its obtained knowledge in order to achieve predefined objectives; and to learn from the results obtained.

NOTE: This is the current definition as given in [i.1].

Operational Database Information (ODI): information held in a centralized or distributed database that may be accessed by reconfigurable equipment during its operation and which may affect the conformity of the reconfigurable equipment to the applicable legislation

RadioApp: software component to be installed and operated on reconfigurable Mobile Devices

NOTE: The operation of the software component impacts the conformity of the reconfigurable equipment to the applicable legislation.

Reconfigurable Equipment: part of a reconfigurable radio system

NOTE: The Reconfigurable Equipment is capable of being dynamically reconfigured to adapt to a wide range of communications conditions. Such reconfiguration may include the band of operation, the radio access technology, the associated networks and the services accessed. The reconfiguration may occur after initial sale deployment and operation.

Reconfigurable Radio System: generic term for radio systems encompassing Software Defined and/or Cognitive Radio Systems

RRS Database Information (RDI): information held in a centralized or distributed database which is used in the process of reconfiguration of reconfigurable equipment and which may affect the conformity of the reconfigurable equipment to the applicable legislation

NOTE: The RDI may be used by either, or both, the reconfigurable equipment or the entity directing or verifying the reconfiguration process.

Software Defined Radio (SDR): radio transmitter and/or receiver employing a technology that allows the RF operating parameters including, but not limited to, frequency range, modulation type, or output power to be set or altered by software, excluding changes to operating parameters which occur during the normal pre-installed and predetermined operation of a radio according to a system specification or standard

NOTE: This is the current definition as given in [i.1].

User: user of the Reconfigurable Radio System or the Reconfigurable Equipment

3.2 Abbreviations

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

CE	Conformité Européenne
CoC	Certificate of Conformity
CRS	Cognitive Radio System
DoC	Declaration of Conformity
EC	European Commission
GSM	Global System for Mobile Communications
HW	HardWare
MNO	Mobile Network Operator
NRA	National Regulatory Authority
OD	Operational Database

ODI	Operational Database Information
OEM	Original Equipment Manufacturer
PAMR	Public Access Mobile Radio
PMR	Professional Mobile Radio
PPDR	Public Protection and Disaster Relief
R&TTE	Radio and Telecommunications Terminal Equipment
RAT	Radio Access Technology
RCP	Regulatory Certificate Platform
RD	Reconfiguration Database
RDI	RRS Database Information
RE	Reconfigurable Equipment
RMP	Reconfiguration Market Platform
RRS	Reconfigurable Radio System
SDR	Software Defined Radio
SM	Software Manufacturer
SP	Service Provider
SW	SoftWare
TCAM	Telecommunication Conformity Assessment and Market Surveillance Committee

4 Principles and Objectives for Reconfigurable Equipment

The present document focuses on the Use Cases and the related procedures applicable to equipment to be placed on the market that is able to be dynamically reconfigured. This includes, for instance, a piece of equipment that can be reconfigured after deployment with new software remotely by automatic means and generally without detailed human interaction. Very often such a reconfiguration may occur "over-the-air" while the reconfigurable equipment is attached to an MNO's network. In the framework of the present document, it is assumed that equipment reconfiguration may include software provided by third party software suppliers. A corresponding legal framework is under development in Europe in the form of the revised R&TTE Directive [i.2]. Other regions may have specific legal frameworks for placing on the market and/or putting into service such reconfigurable equipment.

Herein, it is assumed that methods and processes traditionally used in the context of the conformity to applicable legislation for reconfiguring, updating or revising equipment, often involving human interactions and with the equipment out-of-service during reconfiguration, may continue to be applied to future reconfigurations of such equipment.

The extensions and standards for dynamically reconfigurable equipment may take into consideration the following principles and objectives:

i) Suppliers of third party software which is intended to be installed on identified reconfigurable equipment will ensure and declare that the resulting combination is in conformity to the applicable requirements.

ii) Suppliers of third party information, such as an operational database or a reconfiguration database, which is intended to be used by identified reconfigurable equipment will ensure and declare that the resulting combination is in conformity to the applicable requirements.

iii) A mechanism may be developed to ensure that reconfigurable equipment will only allow compliant software to be installed and to ensure the externally verifiable integrity of the software. The mechanism could be based on a form of electronic marking of the software. The electronic marking may be used to indicate that the software has been certified for compliant operation with the equipment in question. In some cases, specialized hardware and software may be used in order to verify the marking in a trusted way before the software is installed.

iv) Third party software may be installed as long as the resulting combination of software and hardware is in conformity with the appropriate applicable legislation.

v) Manufacturers of equipment should not be responsible for conformity and interoperability testing of third party software or appropriate database information after initial manufacture and sale.

vi) Network operators should not be responsible for i) conformity and ii) interoperability testing and iii) accepting all third party software or database information into their networks after initial deployment and subscription.

vii) As reconfigured radio systems may have an impact on the radio performance of the network and as Mobile Network Operators (MNO) are responsible for customer services and support, there is a need for MNOs to provide and maintain information on what reconfigured mobile devices and software are used in the network and the relevant database that declare the conformance for the combinations of reconfigurable mobile device hardware and software. From an offline perspective, the database should include the general and MNOs specific requirements. From an online perspective, it is necessary for the MNOs to track the potential impact to the network of such reconfigurable equipment including mobile devices.

viii) A history file should be kept inside the dynamically reconfigurable equipment of previous reconfigurations. This may potentially enable the equipment to go back to a previous configuration in case of interference or at least to identify which software modifications have been brought to the equipment (so as to facilitate *ex-post* equipment monitoring).

5 Stakeholders and Interrelations

The ability to dynamically reconfigure equipment throughout its lifetime is important to enable the rapid and economical upgrading of equipment after initial deployment while at the same time assuring the continued conformity to all the applicable rules and the applicable legislation. It is through providing a climate of dynamic re-configurability that the economic benefits of Cognitive Radio Systems technology and rapid deployment of new innovative reconfigurable radio systems will be fostered. Such re-configurability will enable systems to be designed for the future and to take advantage of new technology and regulatory developments.

However, while it is important that the dynamic reconfiguration process not hinder the development of new systems, the process should accommodate a wide variety of equipment, be sustainable over decades of regulatory control, be legally sound and be proof against both innocent misuse and malevolent perversion. In some cases, the new declaration of conformity may cover regulations that were not in effect at the time of original certification or involve service aspects that are new capabilities. The reconfiguration may involve not only the radio equipment, but also the associated databases that may be involved in the operation or reconfiguration of the reconfigurable radio system. The reconfiguration may also be performed in a regulatory domain that is different from the initial certification domain and the reconfiguration may affect features that may be regulated differently in different regulatory domains. It can be anticipated, for example, that in a first phase reconfiguration features are likely to be used only within a single regulatory domain. At a later time, the features could be extended to multiple regulatory domains as needed.

It should be understood that the Use Cases discussed in the present document are not about the conformity testing or "certification" of equipment that has been upgraded with new software or databases. All upgrades should first be verified by their developers using testing processes that are already established within the industry that conform to the applicable legislation. The reconfiguration Use Cases that are the subject of the present document address the process of assuring that new configurations for reconfigurable equipment are properly and appropriately loaded and the proper legal responsibility for conformity is transferred to the new configuration providers. The software and equipment design for the new configuration may be tested for conformity through the appropriate entities and as it is done with non-reconfigurable equipment. Once the conformity testing of the new configuration is successful and a new declaration of conformity for the new configuration is issued, the reconfiguration process that is the subject of the Use Cases in the present document may be used to dynamically reconfigure the equipment and to load the new certificate of conformity to the equipment or database when it is reconfigured in the field. This newly installed certificate of conformity becomes the basis for the continued operation of the reconfigured equipment.

Due to equipment life-times and business cycles, the reconfiguration process should accommodate reconfigurations in which the equipment manufacturer, operator or software vendor may no longer be available to participate at the time of recertification or reconfiguration. Reconfigurations may also involve many layers of software or hardware, and some reconfigurations may rely on presumed operation of previously established configurations. Also, due to the large volumes of deployments of consumer devices, the reconfiguration process should be scalable to accommodate (literally) billions of deployed devices and a similar number of possible new configurations. It may not be practical, for example, to maintain a common database of all possible equipment software configurations and the certificates of conformity for each individual device.

This introductory clause outlines key stakeholders and key concepts for dynamically reconfiguring equipment while ensuring its continued conformity/compliance to/with applicable legislation and standards. One of the purposes of the present document is to enumerate some of the practical and technical Use Cases that should be accommodated by the dynamic reconfiguration process. For example, due to the equipment long life-cycles, the configuration process requires care and caution in its design to prevent failures or malevolent perversion. Furthermore, security requirements for the reconfigurable equipment should be considered to ensure trustworthy operation.

5.1 Stakeholders, Entities and Certificates

This clause lists and briefly describes the Stakeholders ([S]) and Entities ([E]) involved in the illustrated reconfiguration Use Cases as well as the "Certificates"([C]). Not all of the listed stakeholders are involved at the same time.

- **Reconfigurable Equipment (RE) [E]:** equipment that is dynamically reconfigurable through software reconfigurations that may be acquired from a Reconfiguration Market Platform (for instance an SP, see below). This reconfiguration may occur after the initial sale, deployment and operation of the equipment. In this context, "software reconfiguration" could be any change in software or operational database information that affects the RE's operation that may affect conformity/compliance to/with regulations or associated standards. This may include, for example, changes in the radio operating parameters, new spectrum bands, new RAT formats, service features or higher level applications that might affect the RE's ability to provide network services. There may be multiple classes of reconfiguration software affecting different areas of an RE's operation or conformity.

  In some cases the reconfiguration may include the use of specialized hardware modules. The hardware modules may enable the integrity checking of the reconfigurable equipment software and information from operational or reconfiguration databases in order to ensure the loading and installation of reconfigurable components are done in a trusted manner.

  In some situations, the reconfigurable equipment may be physically fixed in location and linked to a communications network (Mobile network base stations are an example of such equipment). In other situations, the reconfigurable equipment may be mobile or in no specific location and linked to communications networks through temporary means such as radio links (User mobile equipment are an example of such equipment). The reconfiguration of fixed and mobile RE may adopt different procedures for dynamic changes. In some cases the RE may be reconfigured using procedures that have previously been used which may, for example, involve human interaction.

- **Reconfigurable Equipment User [S]:** user making use of Reconfigurable Equipment to access services from an SP or to otherwise communicate with equipment that is complaint with the applicable legislation.

NOTE 1: In some cases RE Users may select reconfiguration software components to alter the capabilities and services of their RE.

NOTE 2: Such other communication may include, for example, a private network or a local individual communication.

- **Service Provider [S]:** an SP delivers radio access and network services using equipment including RE. The SP may, for example, be a network operator using licensed spectrum, but may also be a personal or local area network manager. There may be multiple SPs associated with mobile RE through roaming or other commercial arrangements. The SP network may be a public service or a user restricted one (e.g. PMR, PAMR, PPDR network). The SP may require a certificate of conformity, or subscription, for mobile RE to access its network and services. The SP may perform reconfiguration of its network RE, perhaps in concert with the RE's OEM. The SP may also provide the RE User with information on available reconfiguration software (i.e. the SP may also be a 'Reconfiguration' Market Platform provider).

- '**Reconfiguration' Market Platform [E]:** RMP is a Platform where reconfiguration software is advertised and can be downloaded by RE Users in a trustworthy way. The 'Reconfiguration' Market Platform may also inform the RE Users of new, updated or discontinued (no longer supported) software configurations. There may be multiple 'Reconfiguration' Market Platforms which may, or may not, be associated with an equipment or a software provider or an SP. In this context, reconfiguration software refers to software that affects the conformity of the RE to radio or service regulations or to the Service Provider's network. The RE may be reconfigured with software from multiple 'Reconfiguration' Market Platforms. In the present document, the RMP is considered to be generic and covers all relevant market channels (such as the SP, a RadioApp store, etc.).

- **Regulatory Certificate Platform [E]:** the Regulatory Certificate Platform dynamically receives and verifies certificates for REs that may be upgrading their software. The Regulatory Certificate Platform may query the RE to verify its hardware and software platform and its current and previous certificates. The RCP may also issue certificates of conformity for reconfiguration software or database information. The RCP may enforce decisions on mobile RE, which may include granting full access to content and services, granting partial access to services, quarantine a device, or provide RE management or remediation.

- **Declaration of Conformity [C]:** the Declaration of Conformity may be made such that the stated version of software or equipment is in conformity with the applicable legislation and standards. The DoC is the basis for creating a Certificate of Conformity that may be attached to the original equipment or to the related reconfigured versions.

- **Certificate of Conformity [C]:** a CoC is provided after successful completion of testing that proves the conformity of the RE to the applicable legislation and standards. The "Certificate of Conformity"(CoC) is the proof that the RE or its reconfiguration is in conformity with all the applicable legislation and it is the basis for the continued operation of the device. In the European context where the R&TTE directive is applicable, the Certificate of Conformity forms the basis for a "dynamic CE mark" for the RE and so includes the name of the entity responsible for the conformity. A new certificate is required anytime a new configuration, including a new firmware release, affects, or may affect, the conformity of the RE or the appropriate database to the applicable legislation. The RE may also contain other additional "security/authentication certificates" that it may use to prove its identity, configuration and integrity of the software and appropriate databases to various platforms that may request verification. The CoC may be considered an electronic form of the manufacturer's or other appropriate entity's (paper) declaration of conformity that is used in the context of the current processes for assuring conformity to the applicable requirements. The CoC, for example, may be prepared as a result of a Declaration of Conformity, that the new version of software or equipment is in conformity with the applicable requirements and applicable legislation.

- **Original Equipment Manufacturer [S]:** OEM develops Reconfigurable Equipment platforms based on user preferences, service requirements, applicable technical regulations or the facilities of the SP. The platform may consist of only hardware, but may also be a combination of hardware and associated software basis and features. After the reconfigurable equipment is shown to be in conformity to the applicable legislation, the OEM creates a certificate of conformity for the equipment. The OEM embeds the certificate in the platform, and the certification may also be entered in the Regulatory Database Platform to enable a dynamic declaration of conformity when the RE is reconfigured. It may be appropriate that, for RE, an initial printed conformity marking (e.g. "CE Mark") on the RE should indicate that it is Reconfigurable Equipment and hence there may be additional dynamic CE certificates embedded internally that are not related to the original printed marking. Note that if the reconfigurable equipment is not operational without appropriate SW, then it cannot be tested for conformity as such testing requires operational equipment including both hardware and software components. For example, for a modem containing a GSM entity (HW & SW) plus a reconfigurable entity, such a modem would require a certificate covering both the hardware and software.

- **Software Manufacturer [S]:** an SM develops Reconfiguration Software or software components to be used on Reconfigurable Radio System platforms supplied by Original Equipment Manufacturers. After the reconfiguration software is shown to be in conformity to the applicable legislation, the software manufacturer creates a certificate of conformity for the reconfiguration software. This may include technical tools to ensure security/authenticity of the reconfiguration software. The certified and authenticated software may be distributed to users through the 'Reconfiguration' Market Platform or other relevant channels (such as the SP, or direct to the RE User, or bundling with HW equipment, etc.).

- **Operational Database [E]:** OD is a centralized or distributed database which contains information that may be used by reconfigurable equipment for its operation and which may affect the conformity of the reconfigurable equipment to the applicable legislation. The OD may be a platform that is external to the RE and that may be dynamically accessed by some RE to assist with the RE's operations. The Operational Database, including its operation and its information content will be tested and certified in conformity/compliance to/with appropriate standards. The Operational Database will be supplied with a certificate of conformity that may be used to verify the authenticity of the Operational Database and the conformity/compliance of its information and functionality with the appropriate standards. This database, for example, may provide information about local dynamic availability of channels or applicable power levels.

- **Reconfiguration Database [E]:** RD is a centralized or distributed database which contains information that may be used by reconfigurable equipment in the process of reconfiguration and which may affect the conformity of the reconfigurable equipment to the applicable legislation. The RD may be used by either, or both, the reconfigurable equipment or the entity directing or verifying the RE's reconfiguration process. The RD may be a platform that is external to the RE and that may be dynamically accessed by some RE to assist with reconfiguration processes. The Reconfiguration Database, including its operation and its information content will be tested and certified in conformity/compliance to/with appropriate regulations and standards. The Reconfiguration Database will be supplied with a certificate of conformity that may be used to verify the authenticity of the Reconfiguration Database and the conformity/compliance of its information and functionality with the applicable legislation. This database, for example, may provide information about compatibility of various combinations of hardware and software configurations and network compatibility. The database information may be used by RE to assist with changes of their configuration.

- **National Regulatory Authority [S]:** NRA is a national body, or other designated authority, responsible for administering and assuring that the RE can be put into service and conforms to the applicable legislation.

6 Reconfiguration generic Use Cases

There are a number of possible generic Use Cases for the initial certification and subsequent reconfiguration of reconfigurable equipment after its initial certification and deployment. The initial certification Use Cases follows closely the procedures for non-reconfigurable equipment with the addition of the concept of a dynamic certificate of conformity. This certificate may have an electronic format that enables it to be loaded in the reconfigurable equipment and reloaded as part of the reconfiguration process.

The reconfiguration Use Cases typically involve changes in software for the equipment or databases associated with the reconfigurable equipment. To assure that the equipment remains in conformity with the applicable legislation a form of dynamic re-certificating may be required. This may include the additional distribution to the equipment of new certificates of conformity. The new certificates may provide evidence of compliance to the applicable standards and other requirements that may be necessary for access to the Service Provider's network.

There are 7 basic Use Cases:

1) OEM establishing initial conformity of reconfigurable equipment platform.

2) Certificate verification of reconfigurable equipment.

3) Establishing conformity of reconfiguration software.

4) OEM upgrade of reconfigurable equipment (individual or en-masse).

5) Third party upgrade of reconfigurable equipment (individual or en-masse).

6) Configuration enforcement of reconfigurable equipment.

7) RE discovery of databases.

These Use Cases are discussed generically in this clause. Further details are provided in clause 8.

6.1 OEM Establishing Initial Conformity of RE Platform

The establishment of the initial conformity and certification of the reconfigurable equipment platform by the OEM is illustrated in Figure 1. This Use Case is very similar to the conformity testing and declaration of conformity certification that is currently used for non-reconfigurable equipment. As shown in Figure 1 the following steps can be identified:

1) The OEM designs and develops the RE platform.

2) The RE is then tested, for example, by the OEM and the SP for conformity to applicable legislation and standards and a declaration of conformity is made.

3) From the DoC, the OEM creates a Certificate of Conformity for its conforming RE.

4) The certificated RE may then be placed on the market. In the present document, *certificated equipment* relates to RE for which a Certificate of Conformity exists.

In the case of RE, the Certificate of Conformity may be electronically installed in the equipment so that the conformity and compatibility may be verified during operations after deployment. The certificates that are relevant for or associated with the RE should be visible or accessible in the appropriate databases and in the RE. The same should be the case for pre-installed SW combination in order to make sure that it is an operational RE.

Figure 1: Use Case in which OEM develops, certifies conformity and deploys an RE platform

6.2 Certificate Verification of reconfigurable equipment

The Use Case for the verification of a Certificate of Conformity of a given deployed reconfigurable equipment is illustrated in Figure 2. The following steps can be identified:

1) To verify the conformity of the equipment deployed, the inquiring party queries the RE to request its certificate of conformity.

2) The RE replies to the requestor with its current certificate (or certificates).

3) The requestor receives the certificate (or certificates).

4) The requestor verifies the authenticity of the RE's certificate to assure the conformity of the RE (including its conformity for operation in the current location and/or current SP's network).

Figure 2 shows the NRA as the source of the query for certificate verification but a similar request for verification could come from other stakeholders as well. For example, the OEM or the software manufacturer could query the RE's certificate(s) to determine the current configuration of the RE before deploying new reconfiguration software or to ascertain the RE's capabilities.

This Use Case also enables, for example, the SP to query the RE's certificate before allowing attachment to their network or offering specialized services. Such a query would confirm that the reconfiguration SW is approved by the SP before delivery and installation to the RE. Such reconfiguration SW may need to be approved by the SP before being allowed to be installed in the RE. Such a query may also be used by the SP's network to confirm the RE's configuration before allowing the RE to join the network.

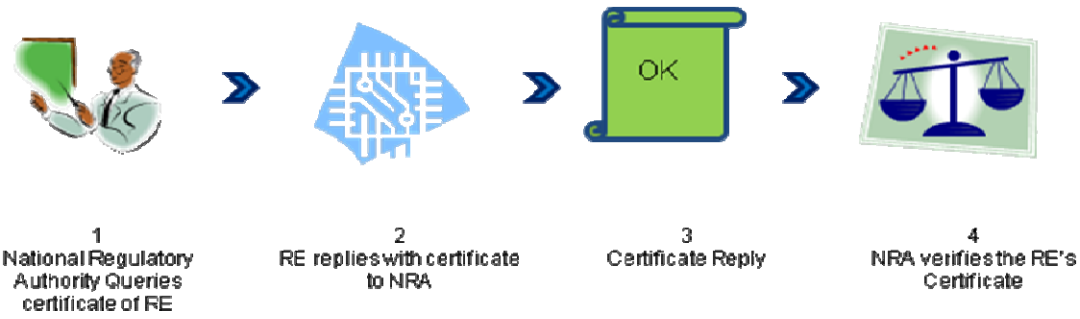


Figure 2: Use Case in which an NRA verifies Certificate of Conformity for RE

6.3 Establishing conformity of reconfiguration software

The Use Case for establishing the conformity of reconfiguration software or software components for RE is illustrated in Figure 3. The following steps can be identified:

1) The Software Manufacturer develops reconfiguration software for applicable reconfigurable equipment together with a list of compatible REs.

2) The reconfiguration software is tested by, for example, the software manufacturer and the SP for compatibility and conformity/compliance to applicable legislations and standards for operation on the stated reconfigurable equipment and networks. With successful testing, a Declaration of Conformity (DoC) is made.

3) From the DoC the software manufacturer creates a Certificate of Conformity (CoC) and a compatibility list for the conforming software product.

4) The certificated reconfiguration software may then be placed on the market.

This Use Case is very similar to the one on initial OEM conformity (described in clause 6.1) with the addition of the compatibility information list associated with the certificate.

Figure 3: Use Case in which Software manufacturer develops and certifies reconfiguration software

6.4 OEM Upgrade (individual or en-masse)

In some Use Cases, the reconfiguration components (e.g. software) may be developed by a team that includes the original equipment manufacturer and the holder of the initial certificate of conformity under which the equipment was initially marketed. This Use Case may include, for example "bug fixing", SW Upgrades, new features and enablement of new technologies such as new radio access technologies or new frequency bands of operation.

The Use Case in Figure 4 considers the case when multiple REs are loaded with a new software by the OEM. The following steps can be identified:

1) The OEM team develops the new SW for the reconfigurable equipment.

2) The new SW is tested for conformity and for compatibility with the intended RE platforms and software configuration and a declaration of conformity is made.

3) From the DoC, the OEM team creates a Certificate of Conformity together with the compatibility list.

4) As part of the distribution of the new configuration to the individual REs, the new components are verified for compatibility with the RE platform.

5) If the new reconfiguration is not compatible with the RE's current configuration, the new configuration is not loaded by the RE and the RE may continue using its previous SW and certificate of conformity.

6) If the new reconfiguration is compatible with the RE's current configuration, the software components and associated certificate of conformity may be loaded by the RE for its use and the RE operates with the new SW and certificate of conformity.

In some (unfortunate) situations, even though the new software is claimed to be compatible with the RE's current configuration, it may not be compatible in practice due to unforeseen conditions and the RE may become inoperative. In this situation, the RE will revert to its previous configuration, or to a previous "safe" configuration for which it has a valid certificate.

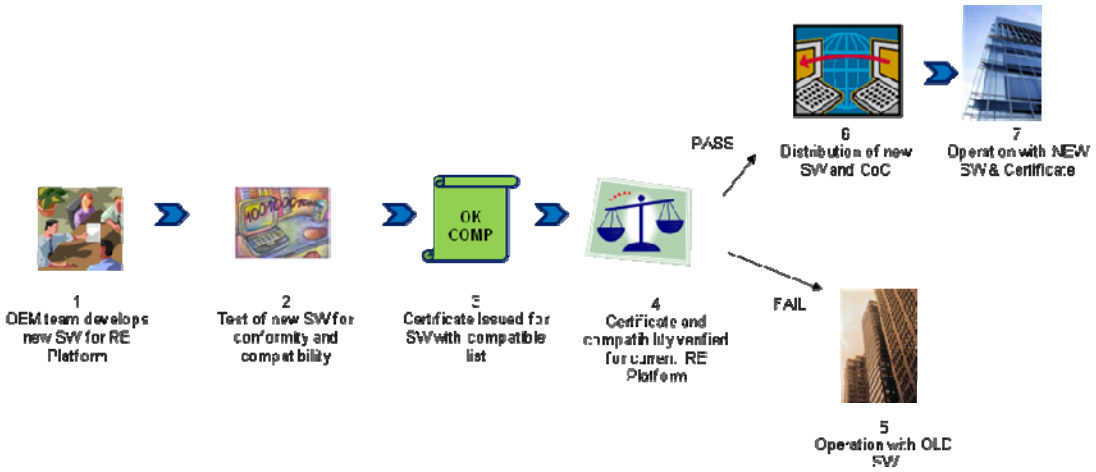


Figure 4: Use Case in which OEM team upgrades applicable reconfigurable equipment en masse

The Use Case outlined in Figure 4 may, for example, be applicable to both mobile and fixed RE. In the case of mobile RE, the verification of compatibility for the RE Platform (step 4) and distribution of new SW and CoC (step 6) may be automatically performed by entities through network connections. In the case of a fixed RE, the verification of compatibility for the RE Platform (step 4) and the distribution of new SW and CoC (step 6) may be performed with human intervention such that the appropriate equipment is reconfigured.

6.5 Third Party reconfiguration (individual or en-masse)

In some Use Cases the reconfiguration components (e.g. software or database updates) may be provided by a team that is not associated with the original equipment manufacturing team that was responsible for the original declaration of conformity. The reconfiguration (new features, SW upgrade, new RAT, operation in a new frequency band, etc) may be directed to all the REs or to an individual RE. It is therefore necessary to establish and verify the compatibility of the new configuration with the RE's current configuration.

This Use Case is applicable when the RE and/or the operational/reconfiguration database(s) are updated. If the database information or protocols that affect the reconfigurable radios are updated, then a new certificate indicating transfer of responsibility to the new team for the database information or protocol updates should be obtained by the reconfigured database.

Figure 5 considers the case when an individual RE is reconfigured "on request". The following steps can be identified:

1) The user requests a new SW for the reconfigurable platform.

2) The SW certificate is verified for compatibility with the RE platform.

3) If the new reconfiguration is not compatible with the RE's current configuration, the new configuration is not loaded by the RE and it may continue using the old SW and certificate.

4) If the new reconfiguration is compatible with the RE's current configuration, the software components and associated certificate of conformity may be loaded by the RE for its use and the RE operates with the new SW and certificate.

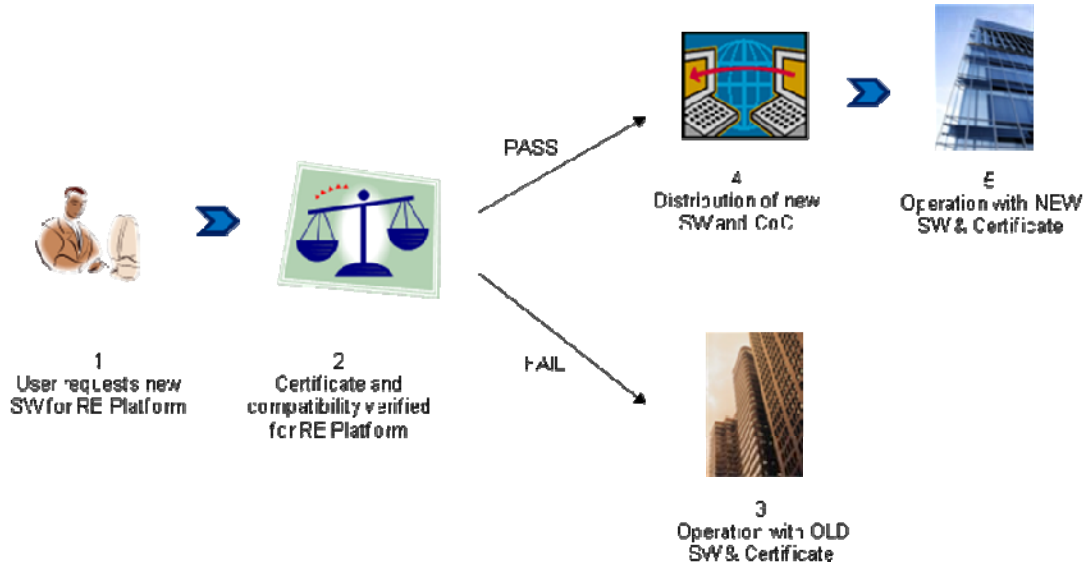


Figure 5: Use Case in which user upgrades SW RE Platform

6.6 Configuration enforcement of reconfigurable equipment

The Use Case for configuration enforcement of reconfigurable equipment (for example to halt an improper operation) is illustrated in Figure 6. The following steps can be identified:

1) The NRA (or another appropriate body) becomes aware of improper operation of an RE. The NRA may be informed of improper operation by, for example, the SP, the OEM, other RE users or other system users.

2) The NRA (or another appropriate body) signals the RE to cease its operations.

3) The RE receives the instructions to cease the current operating mode.

4) The RE ceases its improper functions. This may take place, for example, through a complete switch-off or through a reversion to a previous configuration.

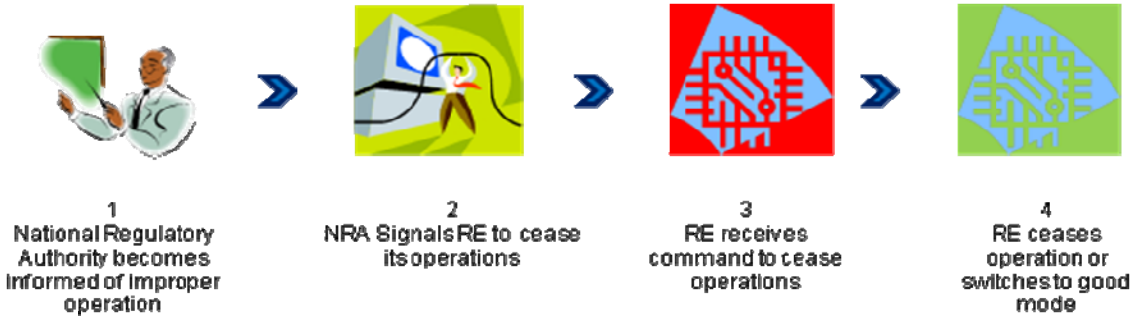


Figure 6: Use Case for enforcement in the event of improper operation of reconfigurable equipment

6.7 RE discovery of operational database (OD) for supporting dynamic reconfiguration of equipment

In some cases the operation of the RE may be dependent on operational information obtained from an operational database (OD) that is external to the RE.

There are many methods by which the initial database discovery and contact may occur. As an example, an initial discovery Use Case is illustrated in Figure 7. The following steps can be identified:

1) The OEM or SW manufacturer embeds in the RE or the reconfiguration software a first link network address.

2) For initial discovery the RE queries the first link network address and includes its current certificate with the query.

3) The first link network address replies with the appropriate operational database network address to the RE.

4) The RE communicates with the operational network database to receive its operational parameters.

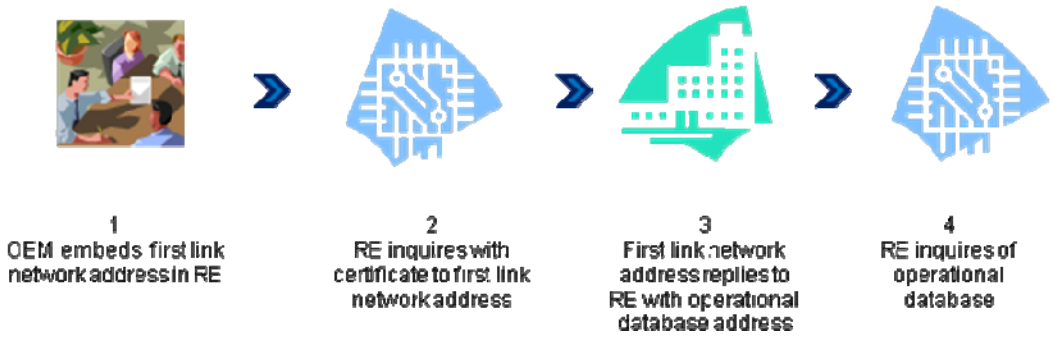


Figure 7: Use Case for discovery of operational database

In this procedure, note that in step 2 the RE includes its certificate in the query so that the first link network address can verify the OD requirements of the RE. In step 3, the response from the first link network address typically will include a means by which the RE can verify the authenticity of the response. This takes place in order to prevent the RE from being directed to a "rogue" OD.

7 Responsibility

7.1 Overview

From a National Regulatory Authority (NRA)'s perspective, a key requirement for reconfigurable radio systems relates to the issue of Responsibility. In the event that an RE does not operate within the regulatory framework, the NRA typically requires that there be a single, easily identifiable, entity (or contact point) that is responsible for the total RE behaviour for conformity.

In some instances the network operator may also require that reconfigurable radio systems conform to minimum network performance requirements and features. To this end, operators also may require that there be a single, easily identifiable, entity that is responsible for the total RE behaviour.

For reconfigurable radio systems in Europe, the TCAM (Telecommunications Conformity Assessment and Market Surveillance Committee) has proposed a definition for two market models - horizontal and vertical markets:

- "**Vertical Market:** all hardware and SDR software which is relevant for the declaration of conformity with the essential requirements for the intended use during the whole life cycle are controlled by one entity."

- "**Horizontal Market:** independent companies placing hardware and SDR software (3rd party SW providers, etc.) separately on the market which, when used together, are subject to declaration of conformity with the essential requirements for the intended use of the equipment."

In the traditional Vertical Market model, the overall responsibility for conformity of the RE remains with the original single entity providing the declaration of conformity. Traditionally, this is the original equipment manufacturer (OEM). However, in case of the Horizontal Market model, there may be multiple entities (other than the OEM) that are responsible for the conformity of the RE and for its consequent behaviour. In many cases these multiple entities may not be aware of each other and an RE may contain multiple reconfiguration software products and its behaviour may depend on the combination of software products loaded and their order of loading. Furthermore, the entity responsible for the original declaration of conformity may not be aware of the reconfigurations of the RE. In the Horizontal Market model there is no single, and easily identifiable entity that is responsible towards the NRA or towards the SP for the total RE behaviour for conformity.

Thus, in the Horizontal Market model it may be advantageous to designate a single entity responsible for the declaration of conformity and behaviour of a RE. It may be noted that in the Horizontal Market model, upon a reconfiguration of the RE, the newly responsible entity may no longer be the original (or previous) responsible entity. It should also be noted that conformity to different regulatory or network operating rules may be required depending on the country of operation and/or the associated network.

The following clauses illustrate some of the interactions between key stakeholders in the Vertical and Horizontal Market case. In clause 7.4, a hybrid model is introduced that combines the Vertical and Horizontal Market approaches into a "Horizontal Market with a single Contact Point". This hybrid combination provides a single, clearly identifiable entity (or contact point) that is responsible for the total RE behaviour for conformity. As a part of the reconfiguration process, the RE is relabelled such that the single Contact Point for the reconfigured RE is clearly identified.

As reconfigurations may lead to a multiplicity of RE variations and conformity contact points (all in similar packages), the original RE marking (i.e. the OEM's original marking) cannot be used to identify the contact point for a new configuration. Some RE may remain unmodified while others will have different combinations of reconfigurations and thus a means to easily identify the responsible contact point for each individual RE is needed.

7.2 Vertical Market model

In the case of the Vertical Market model, a single entity develops the product RE and is responsible for declaration of conformity with the applicable requirements for the intended use and the network compatibility for each reconfiguration during the whole life cycle. Typically, this task is performed by the Original Equipment Manufacturer who controls both new hardware and software components and their possible reconfiguration during the lifetime of the product. This model is illustrated in Figure 8 where the OEM, the RadioApp store and the Software Manufacturer are considered to be one entity.

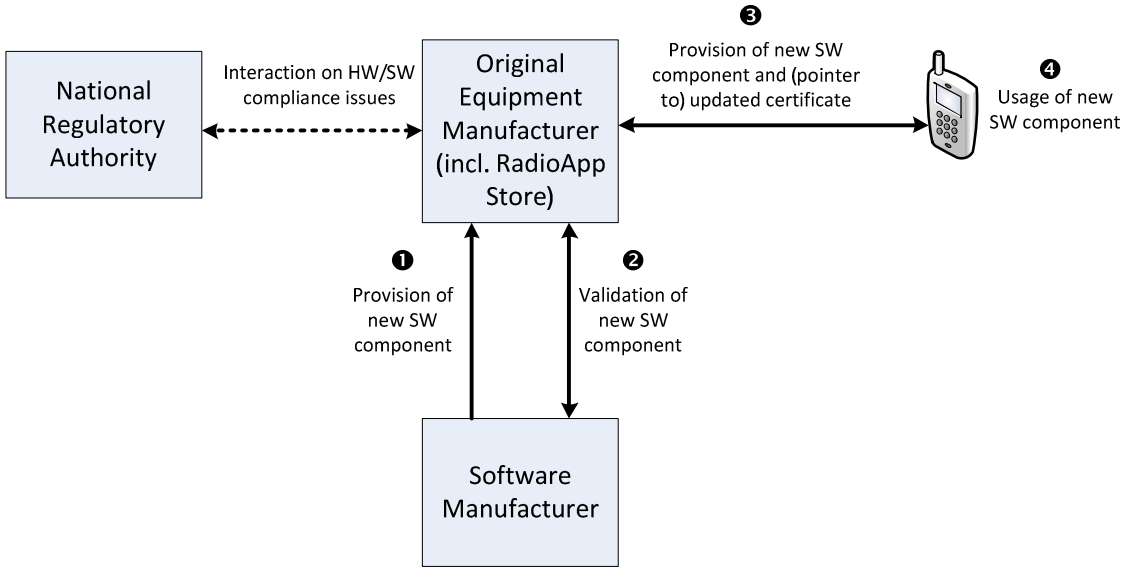


Figure 8: Key interactions in the Vertical Market model

In this model, responsibility clearly remains with the Original Equipment Manufacturer, initially and throughout all subsequent reconfigurations. However the Original Equipment Manufacturer controls the development, testing, approval and deployment of all new software components and thus there is not as open a market for software components as in a horizontal market.

The RadioApp store may be maintained by the Original Equipment Manufacturer as part of its enterprise for distribution of Software components.

7.3 Horizontal Market model

In the case of the Horizontal Market model, independent companies may place hardware and software separately on the market. Typically, a Software Manufacturer may develop new software to operate on a previously compliant RE. In some scenarios in this market, the RE may contain many software components provided by many independent suppliers. When used together, somehow, the ensemble of components continue to conform to the applicable requirements and network compatibility for the intended use of the RE. An example of one possible horizontal market scenario in which the hardware and the new software are supplied separately is shown in Figure 9.

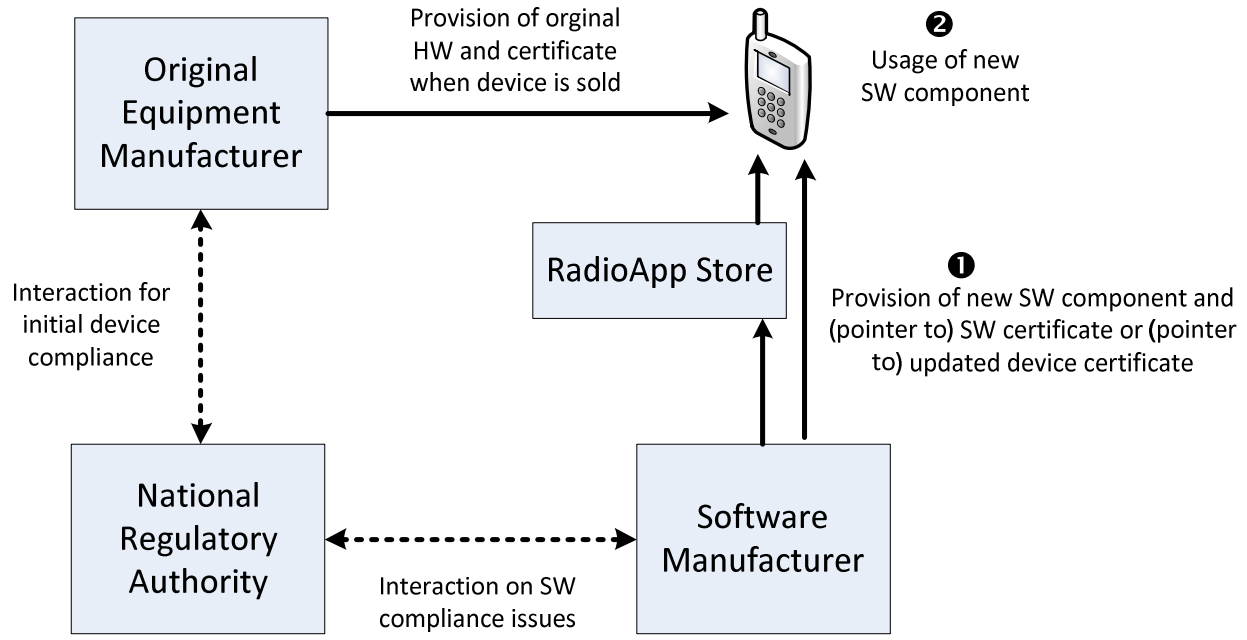


Figure 9: Key interactions in the Horizontal Market model.

The Software Manufacturer may choose to distribute the Software components through a RadioApp Store or directly to the users.

Although this model provides an open market for SW components, there is no longer an easily identifiable single entity that is responsible for conformity and the RE behaviour. As the new components have been installed after initial deployment and perhaps without the knowledge or agreement of the Original Equipment Manufacturer or of the previous entity responsible for conformity, any previous declarations of conformity no longer apply. The OEM, for example, cannot accept responsibility for conformity for REs (Reconfigurable Equipments) that have been reconfigured by third parties without the OEM's knowledge or consent. The NRA and the SP typically require that there be a single point of contact that is responsible for the conformity of the equipment and to resolve issues of surveillance and malfunction. A horizontal market model for reconfigurable equipment without an entity taking over the overall responsibility could therefore be difficult to achieve.

7.4 Horizontal Market model with a single Contact Point

To provide an entity that is responsible for the total RE behaviour for conformity in the Horizontal Market model, a hybrid arrangement may be introduced. The model for a hybrid "Horizontal Market with a single Contact Point" is illustrated in Figure 10. This configuration enables an open market for software components through the use of a "Conformity Contact Entity". The "Conformity Contact Entity" accepts the overall responsibility and liability for the conformity of the reconfigured hardware and software and provides the single Contact Point entity needed by the NRA and the SPs. This single conformity contact point entity for the new configuration replaces any previous contact entity that may have been applicable for the RE. Typically, when the RE is initially sold by the Original Equipment Manufacturer, the manufacturer, or their designate, will be the single Contact Point for the RE behaviour for conformity. When the RE is reconfigured, the Contact Point is changed to the newly designated single Contact Point entity. There may be several mechanisms to designate the new single Contact Point entity.

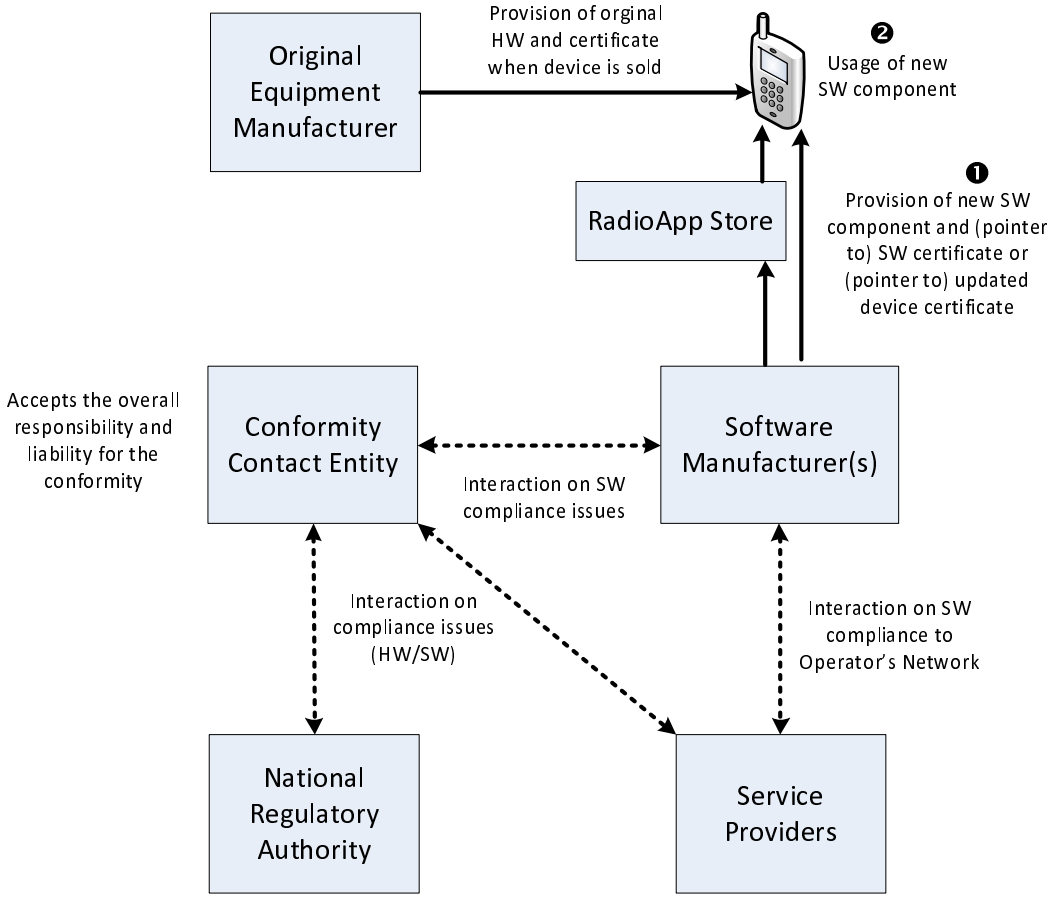
The interaction with the single Contact Point may depend on the roles adopted by the Reconfiguration Software Manufacturer and the Original Equipment Manufacturer. The relationship with the single Contact Point may be one of the example models illustrated in Figure 10 through Figure 13. Other interaction models may also be developed.

7.4.1 Horizontal Market model with an independent single Contact Point

As illustrated in Figure 10, the Original Equipment Manufacturer may take the responsibility as the single Contact Point for conformity and the corresponding certificate(s) at the time when the RE is initially sold. While operated in an unmodified state, the OEM, or their designate, will be the single Contact Point for the RE behaviour for conformity. As illustrated in Figure 10, when new SW components are developed by Software Manufacturers, a Conformity Contact Entity is designated to accept the overall responsibility and liability for the conformity of the RE. This entity provides the single point of contact for conformity needed by the NRA or the SPs for the RE. In Figure 10 the Original Equipment Manufacturer chooses not to be involved in third-party, post-deployment reconfigurations. In the general Horizontal Market it is not mandatory that the Original Equipment Manufacturer participate in the reconfiguration process. In this case, after reconfiguration, the single point of contact for conformity for the RE changes from the previous contact point to the new one. As part of the reconfiguration process the RE is relabelled with its new configuration as well as with its new contact information (e.g. through the loading of a new certificate of conformity as shown in Figure 10).

The Software Manufacturer may choose to distribute the Software components through a RadioApp Store or directly to the users.

As noted earlier in clause 6, and illustrated in Figure 4, in order to assure that the RE is in a suitable configuration for the new software to function correctly, the compatibility of the new software is checked against the compatibility listing of the RE's current certificate of conformity. This may help to assure, for example, that the RE contains suitable base firmware to support the new applications in the new software product.

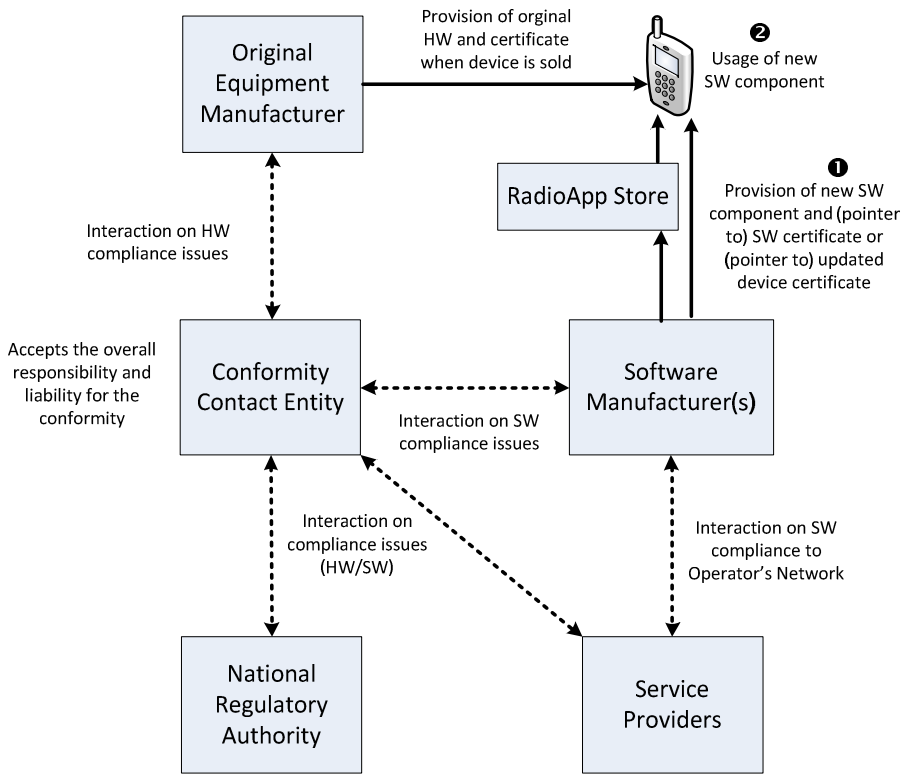


NOTE: In this example, the Original Equipment Manufacturer is NOT involved in the overall reconfiguration process and thus the new Software Manufacturer(s) take the overall responsibility and liability for the conformity of the RE and designate a single Conformity Contact Entity as needed by the NRA(s) and the Network Operator(s).

Figure 10: Basic interactions in the Horizontal Market model with a single Contact Point

7.4.2 Horizontal Market model with an independent single Contact Point and the OEM involved in the reconfiguration

In the Horizontal Market model illustrated in Figure 11, the Original Equipment Manufacturer may take responsibility as the single Contact Point for conformity and the corresponding certificate(s) at the time when the RE is initially sold. While operated in an unmodified state, the OEM or their designate will be the single Contact Point for the total RE behaviour for conformity. When the RE is reconfigured, as illustrated in Figure 11, the Original Equipment Manufacturer may decide to be involved together with the Conformity Contact Entity and the reconfiguration Software Manufacturer in the conformity of the RE. For this reconfiguration, the contact point for conformity issues is assigned to the "Conformity Contact Entity". This entity takes over responsibility for conformity and sorting out the responsibility and liability among the (various) Software Manufacturers. In this model, after reconfiguration the single point of contact for conformity is changed from the previous contact point (for instance the OEM) to the new Conformity Contact Entity. As part of the reconfiguration process the RE is relabelled with its new configuration as well as with its new contact information (e.g. through the loading of a new certificate of conformity as shown in Figure 11).

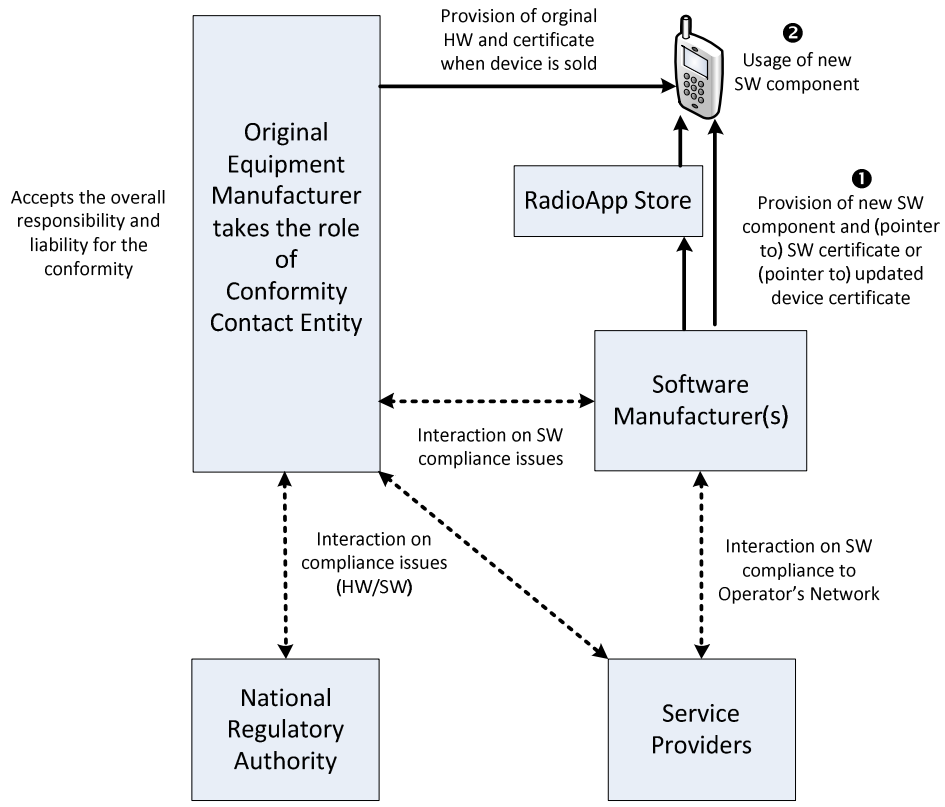


NOTE: In this example, the Original Equipment Manufacturer is involved in the overall reconfiguration process, although the responsibility for conformity of the RE is transferred to the Conformity Contact Entity.

Figure 11: Alternate interactions in the Horizontal Market model with a single Contact Point

7.4.3 Horizontal Market with OEM as single Contact Point

Figure 12 shows an alternative Horizontal Market model where the Original Equipment Manufacturer takes over responsibility as the single Contact Point for conformity and the corresponding certificate(s) even after a reconfiguration of the device takes place. The contact point for conformity responsibility thus remains the Original Equipment Manufacturer. As part of the reconfiguration process the RE is relabelled with its new configuration as well as with its new contact information (e.g. through the loading of a new certificate of conformity as shown in Figure 12).

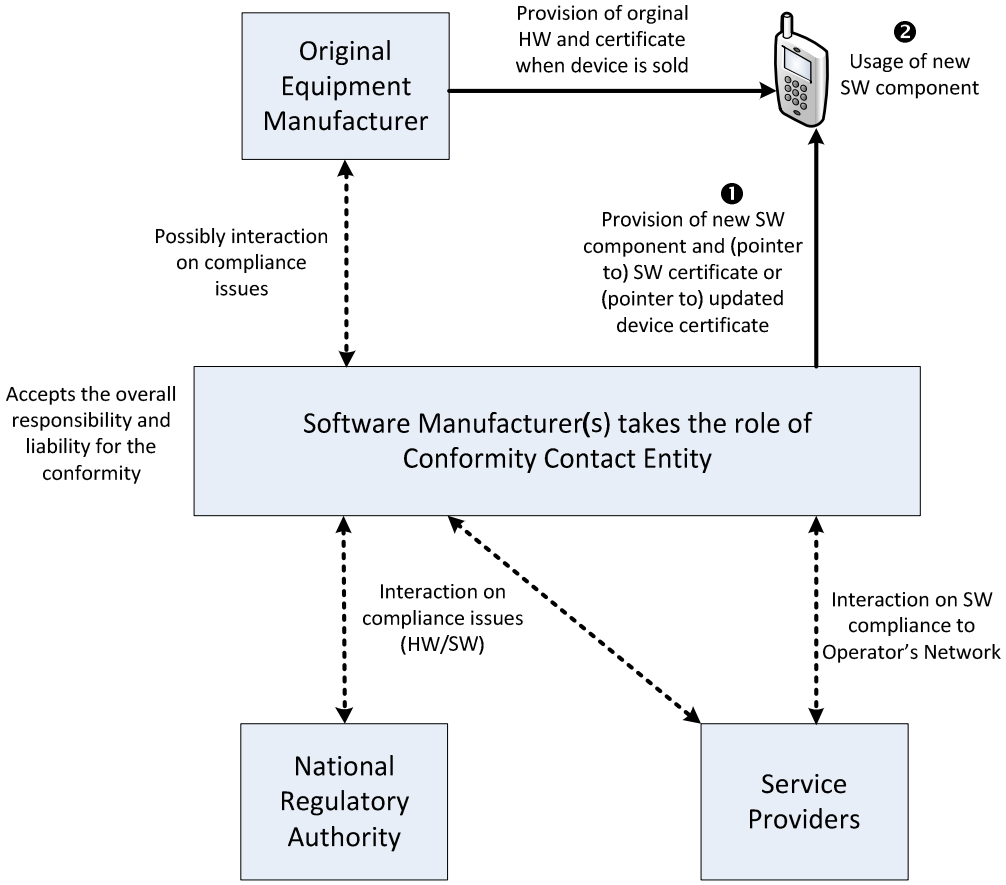


NOTE: In this example the Original Equipment Manufacturer takes over the overall responsibility and liability for the conformity in the overall device reconfiguration process and thus remains Conformity Contact Entity for the device after the reconfiguration. This can be considered to be an extension of the Vertical Market model.

Figure 12: Alternative interactions in the model of a Horizontal Market with a single Contact Point

7.4.4 Horizontal Market with Software Manufacturer as single Contact Point

In the Horizontal market model illustrated in Figure 13, the OEM has initial responsibility as the single Contact Point for conformity and the corresponding certificate(s) at the time when the RE is sold. While operated in an unmodified state, the OEM, or their designate, will be the single Contact Point for the RE behaviour for conformity. When the RE is reconfigured, as illustrated in Figure 13, the Software Manufacturer may choose to take over the role of "Conformity Contact Entity" for the RE. The new contact point for conformity issues thus becomes the Software Manufacturer. As part of the reconfiguration process the RE is relabelled with its new configuration as well as with its new contact information (e.g. through the loading of a new certificate of conformity as shown in Figure 13). In this process, after reconfiguration, the single point of contact for conformity for the RE is changed from the previous contact point (for instance the OEM) to the Software Manufacturer providing the reconfiguration.



NOTE: In this example the Software Manufacturer takes over the overall responsibility and liability for the conformity in the RE reconfiguration process and becomes the Conformity Contact Entity for the RE after the reconfiguration.

Figure 13: Alternative interactions in the Horizontal Market model with a single Contact Point

7.4.5 Horizontal Market model and labelling

With the deployment of the new software reconfigurations in the RE, the NRA and the SPs are informed of the new conformity contact entity for the RE. As each RE may contain a different combination of hardware and software components, each RE may have a different conformity contact entity. In an open horizontal market, the responsibility for the conformity may be assumed by the new conformity contact entity without the knowledge or agreement of the OEM or previous software manufacturers or conformity contact entities. Thus to enable the open market, the RE is relabelled with the new conformity contact entity as it is not the responsibility of the OEM or the previous Conformity Contact Entity or the SPs to keep track of future reconfigurations of each RE.

To facilitate the labelling of the RE with the new conformity contact entity, it may be helpful for the reconfiguration process to install an "electronic/digital label" in the RE. This electronic/digital label (being "machine readable") may be queried by the NRA, the SP or other parties to verify the current configuration of the RE and the current conformity contact entity.

8 Use Cases

8.1 Overview

This clause outlines some detailed Use Cases for dynamically "reconfiguring" the equipment of reconfigurable radio systems (RRS) and associated databases post initial deployment. The Use Cases here described provide further details beyond the description in clause 6, identify key functionalities in the network and equipment entities and illustrate the required interactions between those key entities.

The process for re-configuration has three major phases:

1) **initial** development and certification
2) **operational** reconfiguration
3) **maintenance** query and enforcement of conformity

8.2 Detailed Description of Use Cases

8.2.1 Use Case "OEM Establishing Initial Conformity of RE Platform"

8.2.1.1 General Use Case Description

The **initial development and certification** phase establishes the basis for RE platforms which are maintaining its conformity when they are reconfigured in a post initial deployment. In this initial phase, the initial hardware and associated software are created by the OEM, tested, compliance to the applicable Standards is verified (Harmonized Standards for Europe,) and a certificate of conformity is issued. The determination of conformity can be achieved, for example, in collaboration with an appropriate testing entity. The development may include a variety of expected bands of operation, SP specific configurations, as well as user features and general RE conformity. The initial RE development may also include the basis software by which the RE may be reconfigured. Thus, some aspects of the RE may be utilized for reconfigurations. The initial certificate of conformity becomes a proxy for the authorization for the initial sale and operation of the RE.

A profile of the platform configuration may be maintained by the RE in the form of an electronic certificate of conformity. In this context the certificate of conformity associated with the RE provides information on its current configuration, the history of its reconfiguration and the identification of the entity responsible for the conformity of the RE. The certificate could also be used by an SP to indicate if the RE is suitable for operation in its coverage region.

The process for a dynamic reconfiguration of the equipment is very similar to the process of initial proof of conformity for equipment that is not reconfigurable. The difference being the provision of a certificate of conformity associated with the RE that profiles its initial configuration and that may be updated when there are subsequent, or post deployment, reconfigurations.

8.2.1.2 Stakeholders

The general stakeholder descriptions are outlined in clause 5.1. The following ones are relevant:

- Reconfigurable Equipment (RE);
- Original Equipment Manufacturer (OEM);
- Service Providers (SP).

8.2.1.3 Use Case Description

As illustrated in clause 8.2.1.4, the present Use Case comprises the following key steps:

- The Original Equipment Manufacturer (OEM) verifies the conformity of the newly developed Reconfigurable Equipment (RE) platform and issues a Certificate of Conformity for the RE.-

8.2.1.4 Information Flow

Figure 14 shows the information flow for the Use Case outlined in clause 8.2.1.3.

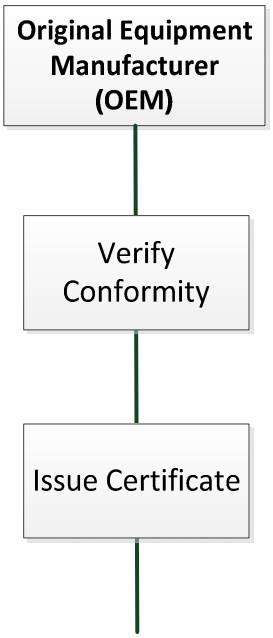


Figure 14: Information Flow for request and issuance of Reconfigurable Equipment (RE) certificate of conformity

8.2.1.5 Derived potential system requirements

Potential system requirements related to this use case are shown in Table 1.

Table 1: Derived potential system requirements for OEM Establishing Initial Conformity of RE Platform

	Functions in the Reconfigurable Equipment	Functions in the Network
Reconfiguration Features	• None	• None
Request/Receipt of Digital Certificates	• Original Equipment Manufacturer (OEM) verifies conformity, a declaration of conformity is made and a Certificate is issued.	• None

8.2.2 Use Case "Certificate Verification of reconfigurable equipment"

8.2.2.1 General Use Case Description

The **maintenance** query and enforcement of conformity phase provides a suitable means for verifying the validity of certificates, which demonstrate that the Reconfigurable Equipment (RE) is operating in conformity to the applicable legislation. Typically, the corresponding query may be triggered by an NRA, the Original Equipment Manufacturer (OEM), the Software Manufacturer, SPs or other relevant stakeholders. In more details:

- An NRA may query the Reconfigurable Equipment (RE) for its current Certificates in order to verify that its current software configuration is in conformity to applicable legislation. While Software typically can only be installed after prior verification of its conformity and compatibility with the RE, a given configuration may not be in conformity to applicable legislation in all regions. The Certificate Verification mechanisms are thus important for Reconfigurable Equipment (RE) that may be operating in various regions.

- The Original Equipment Manufacturer (OEM) and the Software Manufacturer may query the Reconfigurable Equipment (RE) for its current Certificates in order to determine the current configuration of the RE before deploying new reconfiguration software or to ascertain the RE's capabilities. Typically, a Reconfigurable Equipment User (RE User) is only able to acquire and install a new software component after suitable verification of compatibility with the current configuration and Certificate(s).

- An SP may query the Reconfigurable Equipment (RE) for its current Certificates before allowing attachment to their network or offering specialized services. Such a query would confirm that the RE's configuration is compatible with the SP's network. Typically, a Reconfigurable Equipment User (RE User) is only able to acquire and install a new software component after suitable approval by the current SP. Furthermore, when switching to other Networks (in a roaming context, etc.) a verification of the RE configuration and certificate by the new SP may be required.

8.2.2.2 Stakeholders

The general stakeholder descriptions are outlined in clause 5.1. The following ones are relevant:

- Reconfigurable Equipment (RE);
- Original Equipment Manufacturer (OEM);
- Software Manufacturer;
- National Regulatory Authority (NRA);
- Service Provider (SP).

8.2.2.3 Use Case Description

As illustrated in clause 8.2.2.4, the present Use Case comprises the following (alternative) key steps:

- The Original Equipment Manufacturer (OEM) queries a target Reconfigurable Equipment (RE) for a list of the available Certificates. The Reconfigurable Equipment (RE) provides the corresponding information.

- The Software Manufacturer queries a target Reconfigurable Equipment (RE) for a list of the available Certificate(s). The Reconfigurable Equipment (RE) provides the corresponding information.

- The NRA queries a target Reconfigurable Equipment (RE) for a list of the available Certificate(s). The Reconfigurable Equipment (RE) provides the corresponding information.

- The SP queries a target Reconfigurable Equipment (RE) for a list of the available Certificate(s). The Reconfigurable Equipment (RE) provides the corresponding information.

NOTE: These steps do not take place in sequence.

8.2.2.4 Information Flow

Figure 15 shows the information flow for the Use Case outlined in clause 8.2.2.3.

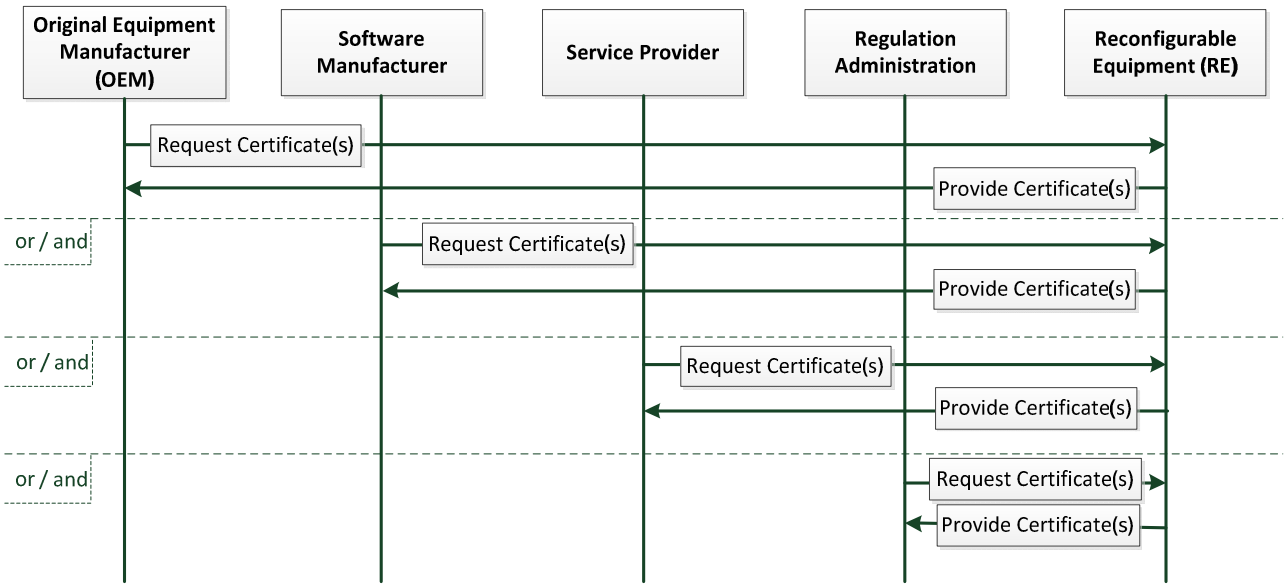


Figure 15: Information Flow for Certificate Verification

8.2.2.5 Derived potential system requirements

Potential system requirements related to this use case are shown in Table 2.

Table 2: Derived potential system requirements for Certificate Verification of reconfigurable equipment

	Functions in the Reconfigurable Equipment	Functions in the Network
Reconfiguration Features	• None	• None
Request/Receipt of Digital Certificates	• Equipment (RE) stores available Certificates. • Reconfigurable Equipment (RE) receives query for available Certificate(s). • Reconfigurable Equipment (RE) provides requested information.	• Transportation of query to concerned Reconfigurable Equipment (RE). • Transportation of corresponding Certificate(s) information to issuer of query.

8.2.3 Use Case "Establishing conformity of reconfiguration software"

8.2.3.1 General Use Case Description

In this Use Case, the establishment of the conformity of reconfiguration software or software components is addressed. This process will support the post deployment installation of 3rd party Software in the RE by ensuring that only verified Software is provided to / installed by RE. The reconfiguration software is developed by a Software Manufacturer and will undergo the following steps:

- The Software Manufacturer develops software for applicable Reconfigurable Equipment (RE) which modifies the radio characteristics of the RE. A list of RE configurations compatible with the reconfiguration software is provided and publicly accessible.
- The reconfiguration software or software components are tested and verified for compatibility and conformity/compliance to the applicable legislation and standards for operation on the RE and networks. Typically, the testing and verification can be performed by an appropriate testing entity, an SP, the Original Equipment Manufacturer (OEM) or similar. In particular, an SP may verify that any 3rd party Software is compatible with a specific SP Network. With successful testing, a Declaration of Conformity is made for the reconfiguration software product.
- From the DoC, the software manufacturer creates a Certificate of Conformity and a compatibility list for the conforming software product.
- The reconfiguration software may then be offered for sale and deployment in the marketplace.

When the new software is loaded in an RE, the new Certificate of Conformity will be also installed in the equipment so that the continuing conformity and compatibility may be verified during further operations and reconfigurations. The new certificate also ensures that the responsibility of conformity is passed, for instance, to the new single contact entity which could, for example, be the new supplier. The compatibility list may be used during the software distribution installation process to determine if the reconfigurable software is compatible with the current configuration of the RE.

8.2.3.2 Stakeholders

The general stakeholder descriptions are outlined in clause 5.1. The following ones are relevant:

- Reconfigurable Equipment (RE);
- Software Manufacturer (SM);
- Service Provider (SP);
- 'Reconfiguration' Market Platform (RMP).

8.2.3.3 Use Case Description

As illustrated in clause 8.2.3.4, the present Use Case comprises the following key steps:

- The Software Manufacturer develops software or software components for a target Reconfigurable Equipment (RE). A list of compatible Reconfigurable Equipment (RE) is provided.
- Reconfiguration software or software components are tested and verified for compatibility and conformity/compliance to the applicable legislation and standards for operation on the stated Reconfigurable Equipment (RE) and networks by an appropriate testing entity, a Service Provider (SP), Original Equipment Manufacturer (OEM), etc. Upon a successful testing, a Declaration of Conformity (DoC) is produced.
- The Software Manufacturer creates a Certificate of Conformity and a compatibility list for the conforming software product.
- The conforming software product is distributed via a 'Reconfiguration' Market Platform (RMP) or other suitable distribution process.

8.2.3.4 Information Flow

Figure 16 shows the information flow for the Use Cases outlined in clause 8.2.3.3.

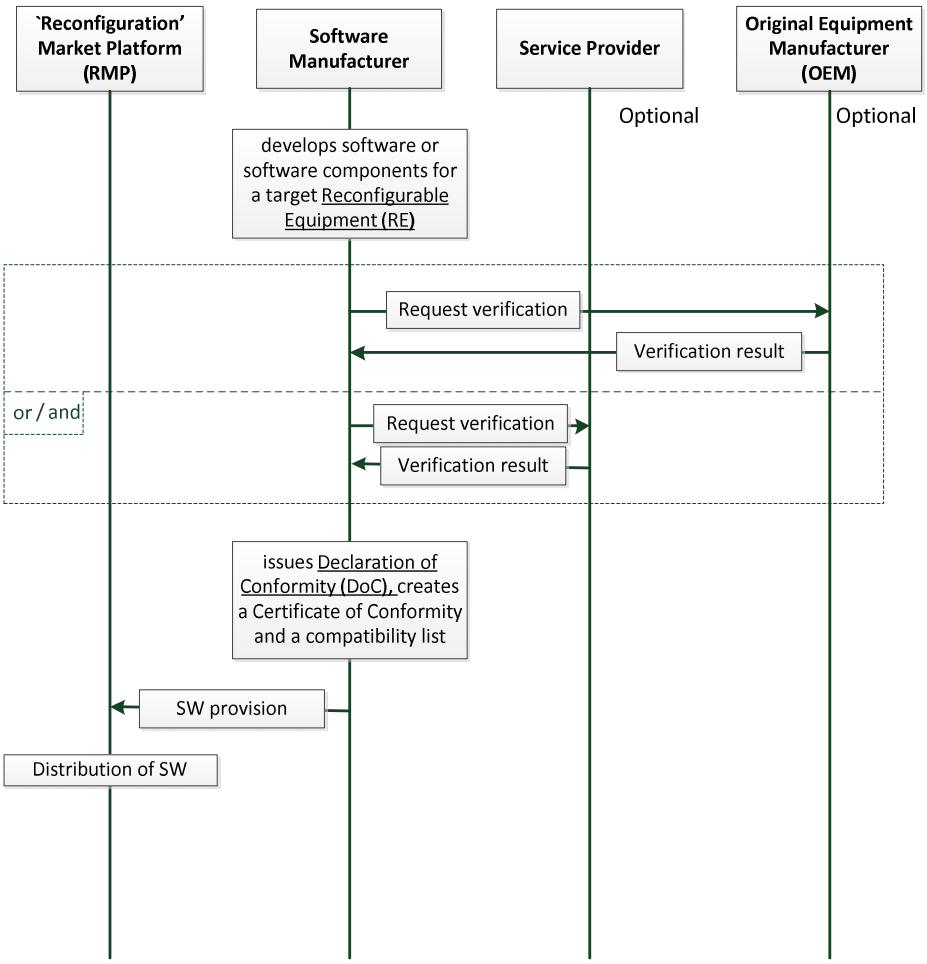


Figure 16: Establishing conformity of reconfiguration software

8.2.3.5 Derived potential system requirements

Potential system requirements related to this use case are shown in Table 3.

Table 3: Derived potential system requirements for Establishing conformity of reconfiguration software

	Functions in the Reconfigurable Equipment	Functions in the Network
Reconfiguration Features	• Acquisition and installation of certificated reconfiguration software.	• None
Request/Receipt of Digital Certificates	• Upon a successful testing, a Declaration of Conformity (DoC) is produced. • The Software Manufacturer creates a Certificate of Conformity and a compatibility list for the conforming software product.	• Transportation of verification requests/results

8.2.4 Use Case "OEM Upgrade (individual or en-masse)"

8.2.4.1 General Use Case Description

The reconfiguration components (e.g. software) may be developed by a team that includes the original equipment manufacturer and the holder of the initial certificate of conformity under which the equipment was initially marketed. This Use Case may include, for example "bug fixing", SW Upgrades, new features and enablement of a new technology such as new radio access technologies or new bands of operation. In this case, the reconfiguration components come from the team that provided the initial OEM certification and may be directed to all the Reconfigurable Equipment or to specific product lines or to individual items of equipment. Once the conformity of the reconfigured equipment is confirmed, a new or revised certificate of conformity is created to be installed in the upgraded RE to indicate the new configuration and to enable compatibility checks with later upgrades.

Figure 17 shows the case when multiple RE are reloaded with new software by the OEM. In more details:

i) The OEM team develops new SW for the reconfigurable equipment.

ii) The new SW is tested for conformity and for compatibility with the intended RE platforms and software configuration and a declaration of conformity is made.

iii) From the DoC, the OEM team creates a Certificate of Conformity together with the compatibility list.

iv) As part of the distribution of the new configuration to the individual RE, the new components are verified for compatibility with the RE's current configuration.

v) If the new reconfiguration is not compatible with the RE's current configuration, the new configuration is not loaded by the RE and the RE may continue using its current SW and certificate of conformity.

vi) If the new reconfiguration is compatible with the RE's current configuration, the software components and associated certificate of conformity may be loaded by the RE for its use and the RE operates with the new SW and certificate of conformity.

Note that in step 0, the compatibility of the new reconfiguration with the RE's current configuration is checked against the compatibility list, and the new software is not loaded if it is not compatible (in which case the RE continues its operation with its previous version).

This Use Case is applicable even if the software distribution is not necessarily intended for all RE. The new distribution may be to individual RE, or it may be distributed en-masse to multiple RE. The new distribution may be for additional features that are chosen by a subset of RE Users, or it may be selected by a SP for a group of its subscribers. The OEM may also develop additional reconfigurable features that may be selected by individual RE Users.

Sometimes the upgrade of the RE may involve changes to the operational or reconfiguration databases (information and/or protocol interactions) that the RE uses to manage its operation. Such a database, for example, could include a geo-location database that is used by RE operationally to manage local channel allocations (OD). In other cases the database may be used by the RE to assist in its reconfiguration process (RD). In some cases, upgrading of the database or its software may also require consequent changes to the dependent reconfigurable equipment such as mobile RE. Consequently, RE upgrades for the dependent RE may also be required. The new certificate installed in the upgraded database indicates its new configuration and may be used by the dependent RE to check compatibility with the upgrades.

8.2.4.2 Stakeholders

The general stakeholder descriptions are outlined in clause 5.1. The following ones are relevant:

- Reconfigurable Equipment (RE);
- Original Equipment Manufacturer (OEM);
- Certificate of Conformity (CoC);
- Service Provider (SP);
- 'Reconfiguration' Market Platform (RMP).

8.2.4.3 Use Case Description

As illustrated in clause 8.2.4.4, the present Use Case comprises the following key steps:

- The Original Equipment Manufacturer (OEM) develops software or software components for a target Reconfigurable Equipment (RE).
- Reconfiguration software or software components are tested and verified for compatibility and conformity/compliance to the applicable legislation and standards for operation on the stated Reconfigurable Equipment (RE) and networks by the Original Equipment Manufacturer (OEM). This test and verification can be performed, for example, through cooperation with Service Providers (SPs). Upon a successful testing, a Declaration of Conformity (DoC) is made.
- If the new reconfiguration is compatible with the RE's current configuration, the conforming software product is distributed via a 'Reconfiguration' Market Platform (RMP) or by the Original Equipment Manufacturer (OEM) or other suitable channel.

8.2.4.4 Information Flow

Figure 17 shows the information flow for the Use Case outlined in clause 8.2.4.3.

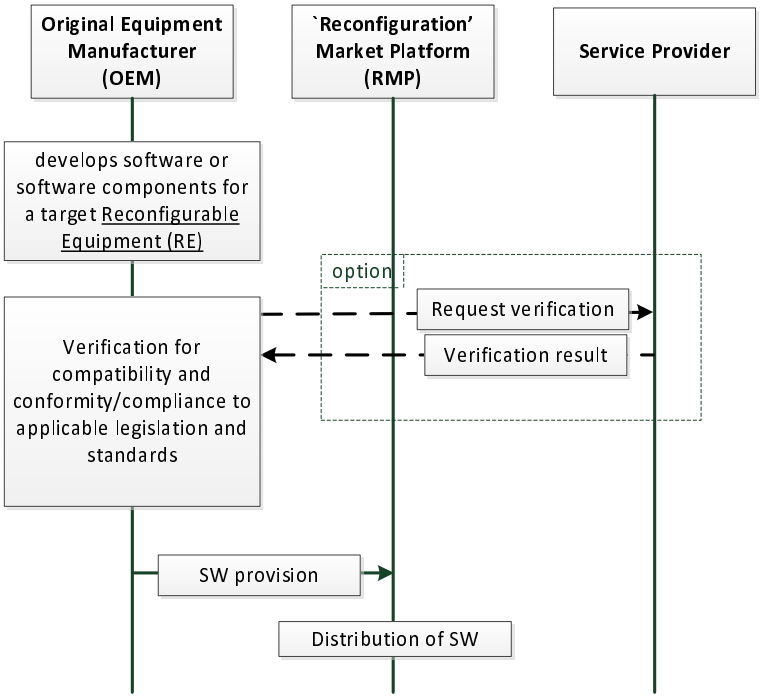


Figure 17: OEM Upgrade (individual or en-masse)

8.2.4.5 Derived potential system requirements

Potential system requirements related to this use case are shown in Table 4.

Table 4: Derived potential system requirements for OEM Upgrade (individual or en-masse)

	Functions in the Reconfigurable Equipment	Functions in the Network
Reconfiguration Features	• Acquisition and installation of certificated reconfiguration software.	• None
Request/Receipt of Digital Certificates	• Upon a successful testing, a Declaration of Conformity (DoC) is produced. • The Software Manufacturer creates a Certificate of Conformity and a compatibility list for the conforming software product.	• Transportation of verification requests/results

8.2.5 Use Case "Third Party reconfiguration (individual or en-masse)"

8.2.5.1 General Use Case Description

Sometimes the reconfiguration components (e.g. software upgrade or database updates) may be provided by a team that is not associated with the Original Equipment Manufacturer that was responsible for the original certificate of conformity. In multiple reconfiguration cases, the reconfiguration components may be provided by a team that is not associated with the team that prepared the reconfiguration software components that have been previously installed in the RE. In this case the compatibility of the new configuration with the RE's current configuration is established.

The reconfiguration components may be directed to all the Reconfigurable Equipment, or to individual RE. In this case, once the reconfiguration components are proved to be in conformity/compliant with the applicable legislation and the associated network configurations, a new certificate of conformity may be issued to the new reconfiguration components (see clause 6.3).

For reconfigurable components that belong to the radio software, it should be noted that the certificate cannot be issued to the individual components. The certificate of conformity is issued to the combination of HW and radio software as a whole. In particular in the case of multiple radio applications the individual device compatibility with the reconfiguration software is verified as part of the reconfiguration process. The compatibility list that is included as part of the certificate of conformity that is created for the reconfigurable software may be used to ascertain the compatibility of the new software with the RE's current configuration before it is loaded in the RE.

If the reconfigurations are compatible with the current configuration of the RE, they may be loaded in the RE together with the new certificate of conformity that will designate its new status and the transfer of responsibility for conformity to the new team.

This Use Case is applicable when either/both the reconfigurable equipment or/and the (operational or reconfiguration) databases are updated. If the database information or protocols that affect the reconfigurable radios are updated, then a new certificate is installed in the database that indicates transfer of responsibility for conformity.

Figure 18 shows the Use Case with an individual RE "third party" reconfiguration. In more detail:

i) The user requests new SW for the reconfigurable platform.

ii) The SW certificate is verified for compatibility with the RE platform.

iii) If the new reconfiguration is not compatible with the RE's current configuration, the new configuration is not loaded and the RE may continue using the current SW and certificate.

iv) If the new reconfiguration is compatible with the RE's current configuration, the software components and associated certificate of conformity may be loaded for its use and the RE operates with the new SW and certificate.

8.2.5.2 Stakeholders

The general stakeholder descriptions are outlined in clause 5.1. The following ones are relevant:

- Reconfigurable Equipment (RE);
- Certificate of Conformity (CoC);
- 'Reconfiguration' Market Platform (RMP).

8.2.5.3 Use Case Description

As illustrated in clause 8.2.5.4, the present Use Case comprises the following key steps:

- A Reconfigurable Equipment (RE) requests SW components from an RMP.
- The RMP verifies if the new reconfiguration is compatible with the Reconfigurable Equipment (RE) current configuration and, if this is the case, distributes the requested SW component to the RE.

8.2.5.4 Information Flow

Figure 18 shows the information flow for the Use Case outlined in clause 8.2.5.3.

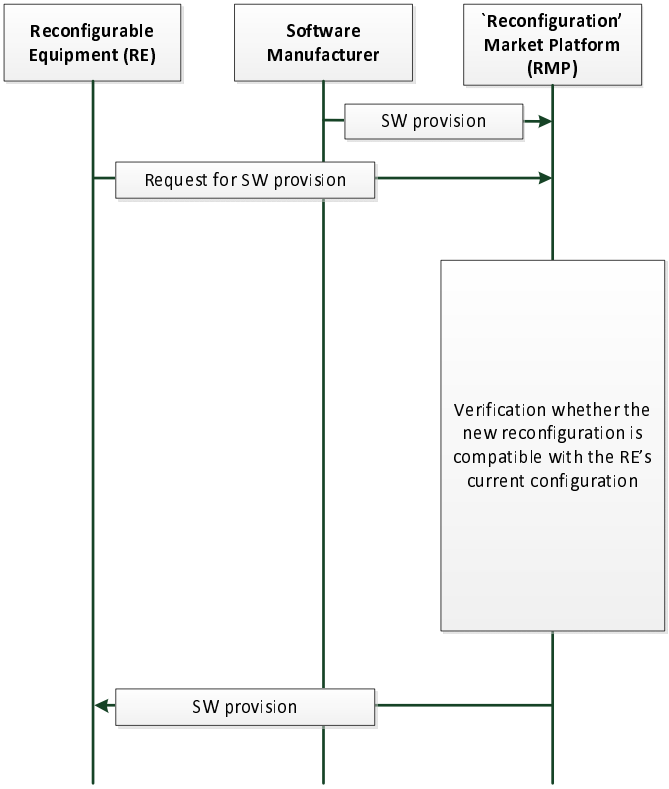


Figure 18: Third Party reconfiguration (individual or en-masse)

8.2.5.5 Derived potential system requirements

Potential system requirements related to this use case are shown in Table 5.

Table 5: Derived potential system requirements for Third Party reconfiguration (individual or en-masse)

	Functions in the Reconfigurable Equipment	Functions in the Network
Reconfiguration Features	• Acquisition and installation of certificated reconfiguration software.	• None
Request/Receipt of Digital Certificates	• None	• Transportation of verification requests/results • Verification of Certificates for the new reconfiguration

8.2.6 Use Case "Configuration enforcement of reconfigurable equipment"

8.2.6.1 General Use Case Description

Configuration enforcement of reconfigurable equipment, for example to halt improper operations, is illustrated in Figure 19. In this case:

i) The NRA (or another appropriate body) becomes aware of improper operation of reconfigurable equipment. The NRA may be informed of improper operation by, for example, the SP, the Software Manufacturer, the OEM, other RE users or other system users.

ii) The NRA (or another appropriate body) signals the RE to cease its operations.

iii) The RE receives the instructions to cease the current operating mode.

iv) The RE ceases its improper functions. This may be, for example, through complete switch-off or by the RE's reversion to a known good operating mode such as a previous software version.

8.2.6.2 Stakeholders

The general stakeholder descriptions are outlined in clause 5.1. The following ones are relevant:

- Reconfigurable Equipment (RE);
- Software Manufacturer
- Original Equipment Manufacturer (OEM);
- Service Provider (SP);
- RE User;
- National Regulatory Authority (NRA).

8.2.6.3 Use Case Description

As illustrated in clause 8.2.6.4, the present Use Case comprises the following key steps:

- The NRA (or another appropriate body) becomes aware of improper operation of Reconfigurable Equipment (RE). The corresponding information is typically provided by a Service Provider (SP), the reconfiguration Software Manufacturer, the Original Equipment Manufacturer (OEM), the Reconfigurable Equipment user etc.
- The NRA (or another appropriate body) signals the Reconfigurable Equipment (RE) to cease its operations.
- The Reconfigurable Equipment (RE) ceases its improper functions.

8.2.6.4 Information Flow

Figure 19 shows the information flow for the Use Case outlined in clause 8.2.6.3.

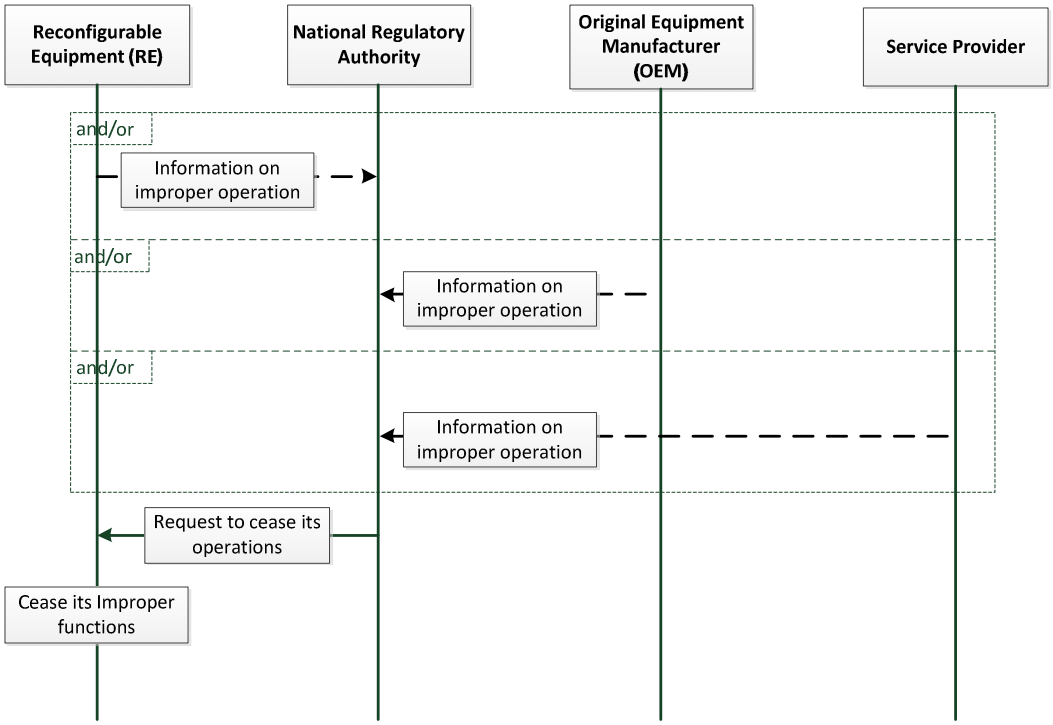


Figure 19: Configuration enforcement of reconfigurable equipment

8.2.6.5 Derived potential system requirements

Potential system requirements related to this use case are shown in Table 6.

Table 6: Derived potential system requirements for Configuration enforcement of reconfigurable equipment

	Functions in the Reconfigurable Equipment	Functions in the Network
Reconfiguration Features	• Cease improper functions.	• None
Request/Receipt of Digital Certificates	• None	• Transportation of information / requests related to improper RE functions

8.2.7 Use Case "RE discovery of an Operational Database (OD)"

8.2.7.1 General Use Case Description

Sometimes the operation of an RE may be dependent on operational information obtained from one or more operational database (OD). These databases, for example, may provide information about local dynamic availability of channels, applicable power levels or geographic information. The RE, when initially deployed or after reconfiguration, will be able to discover and communicate with the appropriate OD(s).

There are many methods by which the initial database discovery and contact may occur. An example of initial discovery is illustrated in Figure 20. In this case:

i) The OEM or SW manufacturer embeds in the RE or the reconfiguration software a first link network address.

ii) For an initial discovery the RE queries the first link network address together with its certificate.

iii) The first link network address replies with the appropriate operational database network address.

iv) The RE communicates with the operational network database.

8.2.7.2 Stakeholders

The general stakeholder descriptions are outlined in clause 5.1. The following stakeholders are relevant:

- Reconfigurable Equipment (RE);
- Service Provider (SP);
- Operational Database (OD).

8.2.7.3 Use Case Description

As illustrated in clause 8.2.7.4, the present Use Case comprises the following key steps:

- The Reconfigurable Equipment (RE) queries a first link network address (typically embedded in the RE or in the reconfiguration software) together with its certificate.

- The first link network address provides the appropriate Operational Database (OD) network address to the Reconfigurable Equipment (RE).
- The Reconfigurable Equipment (RE) communicates with the Operational Database (OD).

8.2.7.4 Information Flow

Figure 20 shows the information flow for the Use Case outlined in clause 8.2.7.3.

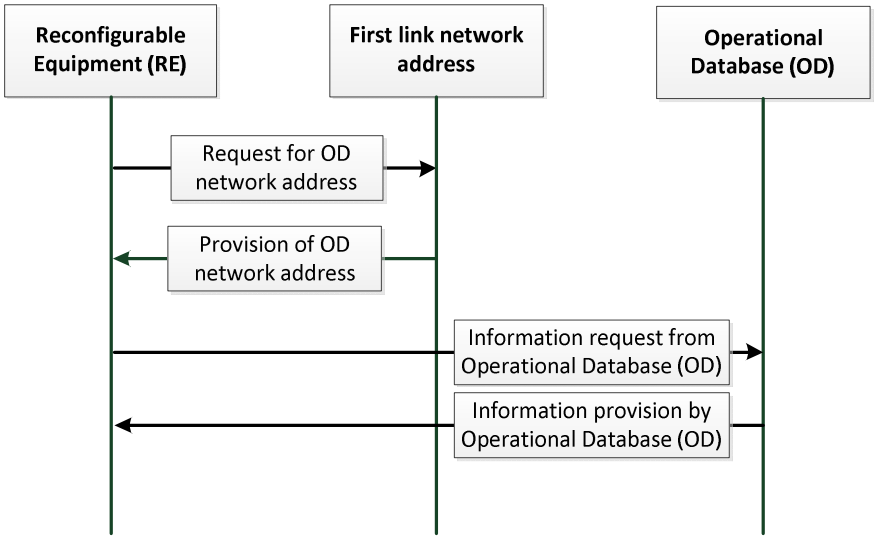


Figure 20: RE discovery of operational database (OD)

8.2.7.5 Derived potential system requirements

Potential system requirements related to this use case are shown in Table 7.

Table 7: Derived potential system requirements for RE discovery of operational database (OD)

	Functions in the Reconfigurable Equipment	Functions in the Network
Reconfiguration Features	• None	• None
Request/Receipt of Digital Certificates	• None	• None

9 Technical Challenges

As noted earlier in Clause 6, and illustrated in Figure 4, in order to assure that the RE is in a suitable configuration for the new software to function correctly, the compatibility of the new software is checked against the compatibility listing of the RE's current certificate of conformity. This may help to assure, for example, that the RE contains suitable base hardware and firmware to support the new applications of the new software product. This compatibility listing, for example, may be stored as a part of the certificate of conformity installed in the RE.

With the deployment of the new software reconfigurations in the RE, the NRA and the SPs are able to identify the single entity that is the point of contact for the conformity of the RE. As each individual RE may contain a different combination of hardware and software components, each RE may have a different conformity contact entity. In an open horizontal market, the responsibility for the conformity of an individual RE may be changed to a new conformity contact entity without the knowledge or agreement of the original equipment manufacturer or previous software manufacturers or conformity contact entities. Thus to enable the open market, the RE is relabelled with the new conformity contact entity as it is not the responsibility of the Original Equipment Manufacturer or the previous Conformity Contact Entity to keep track of future reconfigurations of each RE. To facilitate the labelling of the RE with the new conformity contact entity, it may be helpful for the reconfiguration process to install an "electronic label" in the RE. This electronic label (being "machine readable") may be queried by the NRA, the network operator or other parties to verify the current configuration of the RE and the current conformity contact entity.

10 Conclusion

The present document has identified seven Reconfiguration Use Cases which are the basis processes for the dynamic reconfiguration of Reconfigurable Equipment post initial deployment including features developed by the OEM or by 3rd party Software (components) manufacturers.

1) OEM Establishing Initial Conformity of reconfigurable equipment (RE);

2) Certificate Verification of reconfigurable equipment;

3) Third Party Establishing conformity of reconfiguration software;

4) OEM Upgrade (individual or en-masse);

5) Third Party reconfiguration (individual or en-masse);

6) Configuration enforcement of reconfigurable equipment;

7) RE discovery of operational database (OD).

The proposed Ecosystem enables Equipment to be reconfigured en-mass or individually, so that the RE continues to conform to the applicable legislation and Service Provider requirements. RE users are enabled to acquire Software Components on an individual basis using a mechanism for maintaining continuing conformity for the Reconfigurable Equipment on a per-user basis.

History

Document history		
V1.1.1	March 2014	Publication