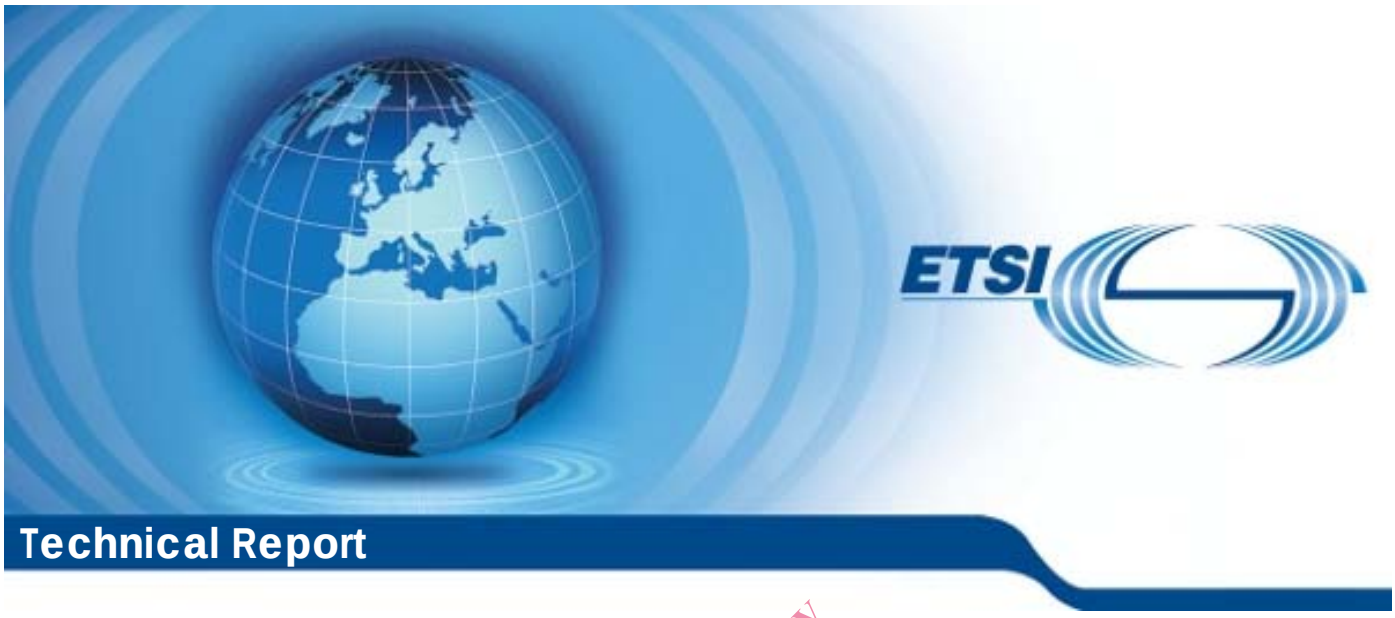
ETSI TR 102 967 V1.1.1 (2014-03)



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

Important notice

The present document can be downloaded from:
http://www.etsi.org

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

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

Contents

Intellectual Property Rights

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