Digital and Dynamic Certification in the Framework of the novel revised R&TTE Directive in Europe

Markus Dominik Mueck
Infineon Technologies AG
IFAG WLS IPA
Am Campeon 1-12, 85579 Neubiberg, GERMANY
Email: MarkusDominik.Mueck@infineon.com

Thomas Haustein
Fraunhofer Heinrich Hertz Institute
Broadband Mobile Communication Department
Einsteinufer 37, 10587 Berlin, GERMANY
Email: Thomas.Haustein@hhi.fraunhofer.de

Paul Bender
Bundesnetzagentur
Canisiusstr. 21, 55122 Mainz, GERMANY
Email: Paul.Bender@BNetzA.de

Abstract— **The next revision of the R&TTE Directive, which represents the basic regulatory framework for wireless communication in Europe, is expected to be finalized in 2011. In particular, this new revision is expected to provide a novel framework for reconfigurable radio devices, for example building on Software Defined Radio features. Those devices may maintain one or multiple links to heterogeneous radio access technologies simultaneously. Also, new features may be added after the sale of the device via software download, such as the addition of a new radio access technology to selected mobile devices. This addition of new features to a device that is already on the market is obviously challenging from a certification perspective. For this purpose, this paper proposes novel approaches for updating certificates building on the novel concepts of dynamic Declaration of Conformity, CE Marking and Alert Symbol marking as they are discussed for example in ETSI Reconfigurable Radio Systems (ETSI RRS) standardization. Those new mechanisms will allow for the software upgrade of features that may affect certification of a mobile device.**

Keywords- Cognitive Radio (CR), R&TTE Directive, Software Defined Radio (SDR)

I. INTRODUCTION

The R&TTE (*Radio equipment and Telecommunications Terminal Equipment*) Directive [1] represents the basic regulatory framework for wireless devices in Europe and is expected to be revised in 2011. During this revision, modifications are expected to be included that will trigger a proliferation of Reconfigurable Radio Systems (RRS) technology. In this framework, the usage of RRS technology is building on two market models: i) In the *Vertical Market Model* framework, one single entity controls all reconfiguration processes and controls available SW components. The provision of novel features, like novel Radio Access Technologies (RATs), may impact device certification. Such a case is currently not covered under the existing regulatory regime and is expected to be addressed in the novel revised R&TTE Directive; ii) In the *Horizontal Market Model* framework, several independent entities can provide software components and the reconfiguration process is not controlled by a single entity – this concept is thus more general compared to the *Vertical Market Model* and is expected to be introduced in a second step. Here, the provision of features, e.g. update of a RATs by 3rd party Software (SW) providers may impact device certification. Again such a case is currently not covered under the existing regulatory regime and is expected to be addressed in the novel R&TTE Directive revision.

The main concern of regulation administrations is typically related to the identification of responsibilities, e.g. in case that a device does not operate following the rules, or in post market surveillance. Both the *Horizontal Market Model* and *Vertical Market Model* are leading to challenges in order to address those requirements appropriately.

In the framework of the ETSI Reconfigurable Radio Systems (RRS) Technical Body (TB), related standardization is ongoing. In particular, [2] illustrates a general Cognitive Radio Systems (CRS) vision related to reconfigurable radio devices. [3] gives a more detailed Mobile Devices (MDs) architecture approach for enabling efficient reconfiguration of such devices, typically based on Software Defined Radio (SDR) concepts. The solution indicated in [3] is expected to provide the technological basis for enabling the introduction of the *Horizontal* and *Vertical Market Models*.

A key challenge of such a novel reconfigurable radio framework lies in certification. Currently, MDs are extensively tested by the manufacturer before being introduced into the market. Also, the manufacturer is typically the responsible entity in case that a MD does not operate in accordance to the essential requirements, e.g. in case that a MD creates unintended interference. In the framework of reconfigurable radio systems under the revised R&TTE Directive regime, this basic approach may change. In particular, it is expected that the new framework will require that a manufacturer includes "*steps*", i.e. hardware components or similar, that allow for example 3rd party SW providers to manage the provision of new SW components

CROWNCOM 2011, June 01-03, Osaka, Japan

DOI 10.4108/icst.crowncom.2011.245858

while being also the final responsible entity for ensuring that a MD operates in accordance to the essential requirements. In such a framework, certification may obviously change over the lifetime of a MD, depending on the SW that is provided after the sale of a device. Consequently, dynamic certification mechanisms need to be introduced. In the framework of this paper, novel digital and dynamic Declaration of Conformity (DoC), CE Marking and Alert Symbol concepts and related signaling approaches are introduced. It is expected that those are elaborated and further discussed in relevant standardization bodies such as ETSI RRS.

The sequel of this paper is organized as follows. Section II introduces a novel flexible radio environment in which MDs may be able to be provided with novel SW components while being already introduced into the market. Section III further introduces requirements related to digital and dynamic Declaration of Conformity (DoC), CE Marking and Alert Symbol marking concepts, which are detailed on a messaging level in Section IV. Section V finally gives a conclusion.

II. NOVEL FLEXIBLE RADIO ENVIRONMENT

In the framework of this paper, a heterogeneous radio environment is considered as illustrated by Fig. 1. Mobile devices are operated in the presence of a multitude of distinct radio systems, typically including cellular RATs, metropolitan area RATs, short range RATs, etc. Moreover, each MD is expected to maintain one or multiple such links simultaneously.

In this environment, it is assumed that a new RAT is introduced while the considered MDs are already in the hands of users. The support of the novel RAT should be enabled by i) provision of related SW components to selected MDs and ii) update of related certification. The provision of required SW components is expected to be rather straightforward, as illustrated by Fig. 1. The SW components are assumed to be finally delivered by a 3rd party SW provider, the handset manufacturer itself or any other entity. The knowledge about the presence of a novel RAT is assumed to be obtained by standard context provisioning mechanisms as they are expected to be introduced in the framework of Cognitive Radio Systems [2,5,6,7]. I.e., a Cognitive Pilot Channel (CPC) Provision entity gathers context information, eventually related to the presence of a novel RAT. This knowledge is communicated to (selected) MDs; those may finally decide to request related SW components in order to be able to maintain links via the novel RAT. The installation of such novel RATs obviously impacts the certification of the concerned MDs. Since they are already deployed onto the markets, this leads to a new situation which was not yet covered under the existing R&TTE Directive regime, but will be addressed under the revised R&TTE Directive. The corresponding responsibility may be taken by the handset manufacturer, which is expected to be in particular the case for the *Vertical Market* model, if it is the handset manufacturer to provide the novel SW components. For the more general *Horizontal Market* model or in case that a 3rd party SW provided is taking the corresponding responsibility, the manufacturer has at least to make sure that suitable "*steps*" are provided such that the device is operated in accordance to the essential requirements.

It is expected that this novel framework will require dynamic certification mechanisms. In particular, novel digital and dynamic DoC, CE Marking and Alert Symbol concepts are needed and will be introduced in the sequel of this paper. Digital and dynamic DoC and CE marking will allow to ensure that the devices operate in accordance to essential requirements in particular in Europe. Also, the corresponding dynamic certificates are straightforward to be verified by a regulatory body in case that a MD crosses the border to another country. Since in other countries, special requirements may be present, this mechanism can be used for example to readjust SW component updates in the various countries; also, it is possible that only specific configurations of SW components are allowed in some countries. The Alert Symbol informs the user about the fact that the configuration of (wireless) features needs to be chosen in alignment with requirements of the concerned country the device is operated in. Parameters like output power levels, available bands, etc. can indeed vary significantly over different (and yet neighbouring) countries. The next section will provide further ideas on how to operate dynamic and digital certification; then, corresponding signaling mechanisms are proposed and discussed.

Business Model Aspects: In order to motivate the discussed framework we would like to look into potential business models behind software upgrades for e.g. additional RATs or RAT features. We consider the following options:

- The MD is prepared for installation of new RATs in order to reduce time to market and cater for a variety of countries the MD is sold to. In this case the MD manufacturer himself or operators of particular countries might have a strong interest in proliferation of this new software component.
- Another option is that operators or network equipment suppliers might use installation of additional software features as a means to offer specific features and functionalities as differentiators for their customers. This concept also includes stepwise activation of software features and belonging functionalities accompanied by a price model allowing pay per feature support as an extension of standard QoS offerings.

It remains unclear how the business model evolves for third party software vendors if the functionality of the MD after installation interferes with rules and strategies of the operator of particular RATs. Does this mean that certificates are also a function of local operator's strategies and following this idea, will operator networks check certificates and approve certain features while others are denied? It has to be clarified how this harmonizes with national and international roaming on one hand, on the other hand this requires on the fly deactivation of certain software features and has to be considered at the beginning for module based software design. Does this require a standardized software modularization?

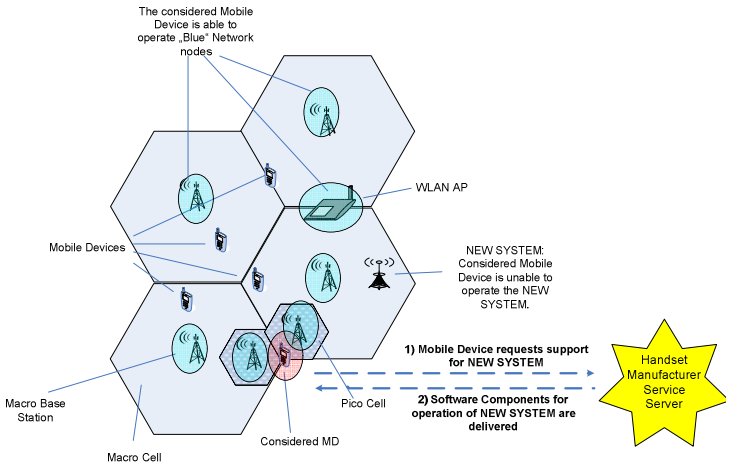

Figure 1: Upload of novel SW components to Mobile Device [4].

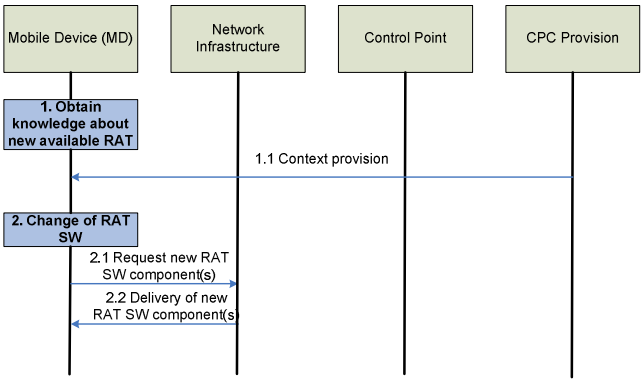

Figure 2: Information Flow for SW component update [4].

Aspects or fail proof installation and activation of software: Another important issue is how to install and activate new software components. Cosinder the case that a firmware update which affects the functionality of RAT and therefore the basic connectivity functions between MD and wireless network is found to be faulty and as a consequence the wireless connectivity is lost after installation and activation. This very simple case illustrates the necessity of procedures for restoring the last successful mode of operation automatically if anything severe goes wrong.

A classic approach to this problem is installation of such new software components similar to firmware updates by connecting the MD via cable with e.g. a laptop, where a software management tool with backups etc is running. In this case a full backup of some or all software components is simple and reliable.

Considering the before mentioned cable option not at hand then mechanisms of automatic reconfiguration into a failsafe old mode is a stringent requirement to be fulfilled by the MD itself and lies therefore in the responsibility of the MD manufacturer.

III. Provision of Novel Digital & Dynamic Declaration of Conformity (DoC), CE Marking and Alert Symbol

In the context of the novel flexible radio environment as introduced in section II, the operational characteristics of a MD can be substantially altered. In particular, a novel RAT may be installed while the MD is already on the market and has been sold to customers – eventually, such a novel RAT may be installed on top of previously installed RATs; in the latter case, the installation order of software components may play a role in the assessment of conformity. After the modification of the MD, in particular the following elements need to be provided dynamically and by digital means:

- The *Declaration of Conformity (DoC)* indicates that a MD conforms with the essential requirements and other relevant stipulations of the R&TTE Directive (currently, a reference is typically given to the release "1999/5/EC" of the R&TTE Directive);
- The *CE Marking* is a mandatory conformance mark on MDs placed on the single market in the European Economic Area. This marking certifies that a product meets EU consumer safety, health or environmental requirements.
- In the case of so-called "Class 2" radio equipment, restrictions may apply when putting it into service (such as an individual license, etc.) and/or placing it on the market. In such cases, the equipment class identifier shown alongside (the "*Alert Symbol*") must be applied.

Since the provision of new software components may require actions related to some or all of the upper markings, a dynamic and digital mechanism needs to be introduced in order to perform this task.

In the framework of this paper, it is proposed to introduce the following novel mechanisms:

1. It is intended that a (or several) new software component(s) is (are) installed on a MD. Before executing the installation, the MD informs a *regulatory database* about the intended final configuration. The order of all previously installed SW components is also communicated to the *regulatory database.*
2. The *regulatory database* searches for available DoC, CE Marking and Alert Symbol certificates, which may have been given by the MD manufacturer or any other suitable entity (such as a certification house, etc.) beforehand. The following cases may occur:

a. If the certificates are available for the intended configuration of the MD, those certificates are communicated digitally to the concerned MD. The MD can install the novel software components, eventually on top of previously installed components.
b. Certificates may only exist for a specific installation order of software components. In particular, such an approach is expected to considerably reduce certification costs in case of a multitude of available software components which may be installed in any order. In such a case, no certificate may exist for the specific installation order requested by the MD; however, a certificate may exist for another installation order. In this case, a digital certificate is given with the request to reinstall all software components in a predetermined order. Once the MD has performed this reinstallation task, it is possible to use the novel feature.
c. In case of a multitude of available software components which may be installed simultaneously, certificates may only exist for the simultaneous operation of some selected software components. Eventually, the novel software component that is intended to be installed on a MD may be incompatible with previously installed software components. In this case, a digital certificate is given with the request to reinstall a selected sub-set of previously installed software components together with the novel software component.
d. Eventually, no certificate is available for the novel software component that is intended to be installed on a given MD. In this case, the *regulatory database* may either decline the request to obtain the required certificates. Then, the considered MD is not able to install and operate the novel software component. Alternatively, the *regulatory database* may request that the MD installs the novel software components in a "*safe mode*" in order to perform a predefined series of self-tests. The results of those tests may then be forwarded to the *regulatory database* which finally decides on the eventual granting of the required certificates.

3. Once the digital certificates are available in the MDs, regulatory entities need to be able to request the concerned certificates from the MDs. This case targets in particular the event that a MD crosses country borders and the responsible regulatory administration changes. The novel regulatory entity may thus request information on installed software components and the respective certificates. If the current configuration is not allowed to be operated in the new environment, the regulatory entity may request to change the MD configuration, e.g. to de-install or de-activate some software components or features.

The interactions between a MD and the *regulatory database* are illustrated in Fig. 3.

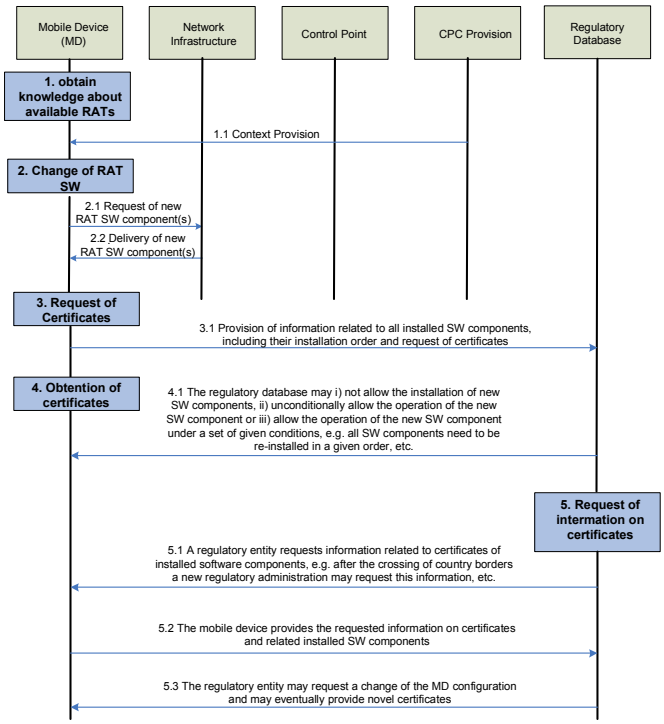

Figure 3: Information Flow for SW component update, including exchange of certificates.

IV. Message format for novel digital & dynamic Declaration of Conformity (DoC), CE Marking and Alert sign

Provided the case that a general software package is requesting digital certification for installation on a MD, we may differentiate between two general options: 1st option: the MD requests certification from the regulation server for the whole software packeage as a one software entity with all embedded features or 2nd otion: the MD request a general certificate for the software package to be installed and operated, but additional certificates might be required for activation and utilization of certain features, which might be operator or country specific.

Considering these two options allows pre-installation of software packages as one certified entity while specific software parts require additional and localized certification for activation. Such an approach can help to reduce software certification procedures tremendously and reduces the risk of coexistence conflicts of software packages provided by different third party vendors.

The message to be sent by the MD to the certification server should include the following details:

- Type of MD, serial number;
- Current firmware status – obtained from the manufacturer;
- Reference code from the software to be certified for installation and operation.

Optional extensions could be:

- Main subscription to local operators (SIM ID);
- Countries the certification is asked for (e.g. pre-installation of features to be used in another country when travelling).

In case a MD tries to enter new network, the operator is interested in obtaining assurance that the new MD asking for wireless network access will behave according to the local requirements and rules set by regulation and the operators own policies.

In order to meet these requirements and considering privacy of the person owning the MD, the network can request the MD to prove that all required certificates are available and valid before granting full access to the network.

The procedure may include the following steps:

1. The concerned MD asks for new network access or network feature;
2. The operator's network triggers the verification of the MD identity and valid software certificates over the central certification database in the internet;
3. The certification database requests specific data and IDs for identification of the concerned MD as proposed above as well as active certificates for software currently installed and/or operated on the MD;
4. After cross-checking these certificate IDs with the database the certification server will inform the operator about pass or failure according to the requested parameters of the software modules;
5. The operator can decide to grant full or limited access to his network or request the regulation server to enforce the disabling of specific software components for this particular network. This particular option is important if MDs are used in another country where different rules apply and certain parts or features of the software cannot be operated;
6. If the procedure is finished the MD has a new specific software setup for the new network and the belonging certification keys. These keys can be exchanged with the network operator in order to assure that only these configurations are active in this particular network.

By these means a flexible, scalable and most important trustful handshake procedure between the MD and the network operator granting access can be established.

V. CONCLUSIONS

The solutions related to digital and dynamic provision of novel software components as detailed in this paper will allowed the controlled provision and installation of such novel software components in MDs. By exploiting these means, manufacturers or 3rd party software providers are for example able to market a MD with a limited set of pre-installed RATs, while further ones can be ordered by the users depending on his requirements. Another promising solution is that a cell phone carrier is able to develop proprietary extensions of the cellular standard; for example, novel 3GPP LTE features can be developed beyond the scope of the 3GPP standard. Then, the concerned carriers can sell those features to interested users who can install and operate the novel features depending on the certificates within the various countries.

Based on the proposed mechanisms and exploiting the novel rules that are expected to be included into the revised R&TTE directive, the provision of such novel software components is organized in a controlled framework and will take into account the requirements of regulatory administrations around the world.

ACKNOWLEDGEMENT

This work is partly performed in the framework of the European-Union funded project OneFIT (www.ict-onefit.eu). The project is supported by the European Community's Seventh Framework Program (FP7). The views expressed in this document do not necessarily represent the views of the complete consortium. The Community is not liable for any use that may be made of the information contained herein.

REFERENCES

[1] 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

[2] ETSI TR 102 802: "Reconfigurable Radio Systems (RRS); Cognitive Radio System Concept", 2009, available at http://www.etsi.org

[3] ETSI TR 102 680: "Reconfigurable Radio Systems (RRS); SDR Reference Architecture for Mobile Device", 2009, available at http://www.etsi.org

[4] ETSI RRS; Reconfigurable Radio Systems (RRS); Definition of refined Scenarios and Use Cases for SDR Reference Architecture for Mobile Device, 2011, available at http://www.etsi.org

[5] Demand driven evolution of the Cognitive Pilot Channel; Mueck, M.; Haustein, T.; Cognitive Radio Oriented Wireless Networks & Communications (CROWNCOM), 2010 Proceedings of the Fifth International Conference on , Publication Year: 2010 , Page(s): 1 - 5

[6] A Local Cognitive Pilot Channel (LCPC) for neighbourhood discovery, relaying and cluster based local cognitive information management; Mueck, M.; Hayar, A.; Cognitive Radio Oriented Wireless Networks & Communications (CROWNCOM), 2010 Proceedings of the Fifth International Conference on; Publication Year: 2010 , Page(s): 1 – 5

[7] Operator governed opportunistic networks: An approach for exploiting cognitive radio networking technologies in the Future Internet, Vera Stavroulaki, Marios Logothetis, Andreas Georgakopoulos, Kostas Tsagkaris, Panagiotis Demestichas, submitted to IEEE Vehicular Technology Magazine