|  |  |  |
| --- | --- | --- |
|  | | **SE43(11)68** |
| 11th meeting of SE43 **Lisbon, 19 – 21 September 2011** | |  |
| Date issued: | 19 September 2011 | |
| Source: | Fairspectrum | |
| Subject: | **Database security and reliability** | |

|  |  |
| --- | --- |
| Summary: | The document presents some possibilities to have max power and other configuration limits for the WS devices in the geo-location database. The reliability and security issues involved are discussed. |
| Proposal: | See chapter 3 Proposal |
| Background: | Report ECC 159 chapter 4 and document SE43(11)24. |

|  |  |
| --- | --- |
| Password protection required? (Y/N) | **N** |

# Introduction

The ECC Report 159 in chapter 4.4 discusses the need to limit the maximum power of WSD devices:

*“It is anticipated that standardisation organisations, such as ETSI, are likely to specify maximum output power for WSDs on the basis of technology limitations or taking into account certain usage models.”*

The matter has also been discussed in input document SE43(11)24 which proposes certain maximum power limits according the device type.

There have been also other opinions expressed that such fixed limits might unnecessarily narrow the possible future innovations and ways of using WS devices. Some other affiliations have expressed their concern about software based limitations based mainly on two issues: the database data may not be correct (or algorithms fail) or that the database data might be erroneous due to malicious hacking.

The purpose of this document is to open a viewpoint for further discussion in order to avoid hard obligatory limits already to be written into the standard.

.

# Use of configuration database

The main idea of this proposal is to use a separate **configuration database** to give the fixed maximum limits or allowed set of values for both the WS devices *AND* the actual spectrum management system. The set of configuration data could include, e.g., maximum allowed tx power, allowed frequencies, geo-location areas, time frames etc.

The configuration database would be such whose content would not be updated frequently and it would be separated from the public network. Also, it would not assume (or allow) anything to be written into it from either the WSDs or from the spectrum management system. The general overview picture is given in Fig. 1.



Figure 1: White space network model including a configuration database.

The general outline of working would be along the lines below:

1. The general limits (configuration data) are written into the configuration database (CS) and the write access is closed. The write rights are confirmed via authentication.
2. The configuration data set is sent to the spectrum management system (SS) where it is also saved.
3. The WS device (e.g. the base station) sends a request to the configuration database (CS) (i.e. permission to use the network in general)
4. The configuration system sends back the configuration set (the allowed set of values) together with a generated unique code (“signature”) that is characteristic for that WSD only.
5. The configuration system also sends the unique code to the spectrum management system, which saves it into a signature pool.
6. The WSD asks the specific permission to send from the spectrum management system (geo-location database) (SS). The request also includes the earlier unique signature code that was given by the CS.
7. The spectrum management system checks first the validity of the code against its pool of codes. If the code is found, it means that request comes from a device which obeys the overall limits set for the network.
8. The SS calculates, using its own algorithms, the actual configuration data for the WSD.
9. The SS checks the calculated data against the general configuration data it has earlier got from the CS. The CS data overrules in case of any conflicts between the calculated data and the configuration limits. The final data set must always fit into the configuration limits.
10. The SS sends the final set of data values back to the WSD.
11. The WSD checks the received values against the configuration data it has earlier got from CS. In case of conflicts the CS data overrules similarly as in point 9.
12. The WS operation starts using the final, checked set of parameters.

The relevant points in the above system are:

* The configuration data (limits) is written via a protected interface with authentication. Between the updates writing is disabled. This should give very good protection against hacking.
* The configuration data is separately transmitted both to the spectrum management system and WSD
* The validity of the transmission parameters is checked twice - once in SS and once in WSD
* The capability of WSD to obey overall limits is checked in SS using unique signatures.

Any human system is prone to errors but careful design can make the probability of malfunctions very low. In the above system by limiting the writing rights, using authentication with secure links in communications and having double checks of transmission parameters as final stages one can reduce the errors to a minimum. It is also clear that the above description just gives some outlines along which the final system would be designed. Especially using various cryptographic and coding methods in various phases to secure the connections, to check the authority of devices and databases and to confirm data reliability could be further developed. These should be subject to further studies.

Modification including hardware limits

It is possible to modify the system described above to include also WS devices with inbuilt hardware limits (e.g. maximum tx power). In such system each WS device is given a unique signature giving an indication that the device has inbuilt hardware limitation. These signatures are registered into the spectrum management system. They could be in the same pool of valid signatures, where also the signatures of the devices with software limits are stored.

This arrangement would allow WSDs with hardware limits and software limits to operate in the same network (or area). The WSDs with hardware limits would request the operational parameters directly from the SS giving in their request the signature they have. These devices would not contact the CS at all. Otherwise the SS operates exactly as already described above. There would not be any additional check of the validity of the parameters in the WS terminals. The WSDs with software limits would also operate as already described above where the parameter sets are checked also in the WS terminals.

# Proposal

Based on the description above and in order to allow maximally flexible use of whitespace systems without compromising the protection of primary services, we propose that the following actions would be taken:

1. Include chapter 2 of this document as annex into the working document SE43(11)40A1 Annex1.
2. We would propose the following text to the chapter 5 “ Technical considerations on the protection of the broadcasting service” of SE43(11)40A1 Annex1:

**“**

**5.4 Use of configuration database**

For maximally efficient use of WS spectrum and not to prevent future innovations it would be beneficial if the maximum transmitting power limits are not set in hardware for all devices. Some or all WSDs could have limits set by software. The overall limits would be fetched from a secure configuration database. This approach might have secured access to modify the configuration data set and have checks of transmission parameters in several places both in the spectrum management system and white space devices. The terminal capabilities would be checked in the system by unique signatures granted by the configuration database. Additional studies about including cryptographic and coding methods to ensure authority and data validity in various phases should be made.

This kind of approach could easily be extended to have a network including terminals with hardware or software limitations. For closer description see annex xx.

“