# Device Authentication Architecture for TV White Space Systems

Jarkko Paavola and Arto Kivinen
Turku University of Applied Sciences
Turku, FINLAND
jarkko.paavola@turkuamk.fi

***Abstract*—Collective use of spectrum refers to a case where spectrum is accessible for independent users at the same time in a particular geographic location under a well-defined set of conditions. One example of collective spectrum use is the communication based on TV white spaces, which is emerging globally. Commercial operation is on-going in the United States and pilots are being deployed in Europe, Asia and Africa. During the operation of TV white space communications devices are not allowed to cause interference towards licensed incumbent uses, which are TV signals and wireless microphones. White space devices query allowed frequencies and transmission powers from the geolocation database. Here, we propose authentication architecture and protocol for two purposes: for the automatic registration for wireless microphones so that they can be protected by the geolocation database, and for the authentication of TV white space devices so that misbehaving use can be prevented. Third benefit of the proposed system is that frequency allocations are registered based on the real usage, which enhances spectrum utilization.**

***Keywords- Collective use of spectrum, TV white space, PAWS, PMSE, wireless microphone, incumbent protection, TPM, authentication, challenge-response protocol***

## I. INTRODUCTION

The need for wireless spectrum is growing fast due to the success of smart phones and tablets. Users demand wireless access everywhere and all the time. Spectrum shortage forces to utilize that scarce resource more efficiently. One of the most prominent approaches is dynamic spectrum use. There, different strategies have been proposed. Collective use of spectrum (CUS) refers to a case where spectrum is accessible for independent users at the same time in a particular geographic location under a well-defined set of conditions. One example of collective spectrum use is the communication based on TV white spaces, which is emerging globally [1].

Traditionally, frequencies are strictly regulated to guarantee that wireless communication systems do not cause interference with each other. But, frequency bands have been also allocated for unlicensed operation. For example, ISM band at 2.4 GHz frequency is used by WLAN and Bluetooth transmissions among other systems. All these systems must be able to cope with the interference caused by other wireless transmissions.

Wireless systems operating in regulated frequencies can assume that other systems are not causing interference. Drawback is that the spectrum utilization is not optimal [2]. Depending on the wireless system there can be substantial temporal and geographical differences how spectral resources are utilized during communications. These locations where the spectrum is un-utilized appear as white areas in the system coverage maps. Therefore they are referred to as *white spaces*. Another terms used in the literature are spectral holes or spectrum gaps.

The transition from analog TV transmissions to digital TV frees up large amounts of frequencies in VHF and UHF bands. This is also called as digital dividend. The competition for digital dividend is hard and for example mobile operators are demanding more spectral resources to provide mobile broadband services. Regulators may allow also cognitive radio technologies to access digital dividend.

Frequencies in VHF and UHF bands are very attractive from the network point-of-view. Propagation properties are good, since the attenuation of signal is slower than with high frequencies. This makes possible to cover large areas with the small amount of base stations, which lowers network building costs.

TV white space (TVWS) is the unused spectrum on TV broadcasting frequencies (470 MHz – 790 MHz) in an arbitrary location [3]. TV white spaces are created especially by efficient spectrum utilization of the digital broadcasting. TVWS is currently the first area that is considered for white space devices (WSD). The reason is that due to the network planning strategies there is available a relatively good amount of white spaces. Also, the TV signal and its coverage area are more stable than for many other communication systems. Wireless microphones are also operating in the TVWS and they should not interfere with TV signals. White space devices have to protect both incumbents: TV and wireless microphones. The incumbent use is also called as primary use while white space utilization is referred to as secondary use in this paper.

In this paper, three operational challenges for the TVWS are considered.

*1) Incumbent devices should be protected by a central database called geolocation database in the context of TV white spaces. Incumbent devices, whose location and time instance when they are used are difficult to predict, are challenging for the centralized database approach.*

CROWNCOM 2014, June 02-04, Oulu, Finland

DOI 10.4108/icst.crowncom.2014.255736

*2) Secondary devices using the shared spectrum should be authenticated to guarantee that only authorized devices are allowed to operate, and to provide information security.*

*3) In the collective spectrum use sharing model, fairness between all spectrum users has to be guaranteed to prevent a single or a few devices from reserving the whole available spectrum.*

As a solution for the aforementioned challenges, this paper proposes security architecture and protocols based on Trusted Platform Module (TPM) chip. Device authentication will address the challenges shown above can be solved with the proposed system as follows: 1) incumbent devices will register to the database automatically; 2) TPM provides cryptographic capabilities allowing encryption and authentication; and 3) frequencies are made available to other secondary users immediately when the device is offline. TPM is cheap alternative that provides hardware level roots of trust.

The system was developed originally for managing wireless microphones automatically. The same procedure can be extended to other wireless communication systems, and required modifications to operate with TV white space systems are shown. In the future, the procedure could be applied to many kinds of dynamic spectrum access technologies, where it is important impose policy enforcement to control when and which devices are allowed to access the shared spectrum.

The rest of the paper is organized as follows: Section II presents TV white space communications and required incumbent protection methods. Information security challenges are also discussed. Section III presents the TPM, which is the basis for the authentication architecture proposal. Section IV discusses incumbent protection in the TVWS while Section V is devoted to the device authentication based on the TPM. The method is applied for wireless microphones, also known as program making and special event (PMSE) devices, and also for white space devices in Section VI. Finally, conclusions are drawn.

## II. TV White Space Communications

The role of the geolocation database [4,5] is to protect incumbent systems, search for available white space frequencies for white space devices, and possibly also control the interference between them. Interference scenarios that must be taken into account are co-channel interference outside the service area of primary system, and the adjacent channel interference inside and outside the service area of primary system. The name geolocation database is used to emphasize the importance of geographical information in the controlling of the utilization of white space spectral resources.

The accuracy and precision of database algorithms are essential in determining frequency channel and transmitting power. The closer is the database output to optimal value for the given location input, the better is the white space utilization. The optimal value means that the white space communications uses the maximum allowable transmission power, while incumbent systems can still be operated normally.

If incumbent system users are over-protected, the amount of white space diminishes rapidly. The over-protection refers to a situation, where the WSD transmission power is set to a lower value than it could be without causing visible or audible interference for the incumbent use.

With geolocation databases also additional information security issues must be taken into account from the different point-of-view than in traditional wireless communication. This is due to the Internet access between the WSD and the database. The device and the database must perform mutual authentication. The database has to know if the device is allowed to access white space. On the other hand, the device has to know which databases are certified by regulatory authorities. Naturally, data transfer has to be encrypted and the integrity of geolocation data has to be secured. The database may be also a target for Denial of Service (DoS) attack. If information security fails, it can cause severe interference to incumbent systems, in addition to white space network, due to the incorrect or inaccurate information on the allowed white space areas or maximum transmitting powers.

In the literature, the vulnerability of TV broadcast network in the case mis-behaving TV white space system has been a concern as the TV is the main source of information distribution in crisis situations. A main consideration in publications with security considerations for cognitive radios and dynamic spectrum access have considered DoS attacks towards secondary networks, and also secondary network as a tool for DoS against primary networks [6-10]. Reference [10] includes also the analysis for white space system susceptibility for man-in-the-middle attack. In [6] analyses also for the fair distribution of spectrum resources between white space devices have been performed.

### *A. PAWS Protocol*

All open protocols for the Internet are defined by Internet Engineering Task Force (IETF), and they are published as RFC documents. For white space communications Protocol to Access White Space (PAWS) [11] definition is expected to be completed during 2014 in the IETF. The protocol defines communication between white space base station/access point and geolocation database.

In the beginning of the definition process, before the actual protocol design, a use case document was set up as RFC 6953. Based on the use cases threat models were derived, which are summarized in the following. Based on the threat model, information security requirements for the protocol were defined. Situations where the PAWS protocol might be used to inflict damage to white space systems include:

- Unauthorized use of the white space system by exploiting vulnerabilities in the base station or the geolocation database.
- The forgery of communication between base station and geolocation database.
- The exposure of the WSD location and identity by eaves dropping.

- The collapse of connection to the geolocation database, which will stop the operation of white space communications.

From the threat description above information security requirements were derived. Requirements are quite traditional for the communications in the Internet: The PAWS protocol must allow mutual authentication, take care of message integrity, guarantee information confidentiality with the encryption, and ensure geolocation service availability. Each requirement can be analyzed in more details for this specific application

Authentication threats:

- User modifies the device so that the geolocation database believes the device to be certified. Replay attack may be possible if external device is able to record registration process.
- A WSD must verify the validity of the geolocation database. If rogue database would be able to feed false information to the WSD, it would cause interference for the primary use.

Integrity threats:

- Forged request e.g. location spoofing from WSD to geolocation database could cause interference to the primary system or other white space devices.
- Forged geolocation database response would cause similar effect as the rogue database.

Confidentiality threats:

- If a device would be able to eaves drop communication it would be able to use white space frequencies without the authorization from the geolocation database.
- Without proper encryption third-party devices could be able to uncover the location and the identity of the WSD.

Availability threat:

- The access to the geolocation database may be prevented by DoS attack, or the loss of Internet connection.

It should be noted that national regulators may impose more strict information security specifications that those considered for PAWS protocol design.

In the discussion above the WSD refers actually to master device, or white space base station. For client, or slave, devices communicating with the WSD authentication is not mandated in the PAWS specification. However, it is possible over TLS protocol (RFC2818). The TLS client authentication procedure only determines that the device has a certificate chain rooted in an appropriate certificate authority (CA). The problem is that the database does not know what the client identity should be, unless it has some external source of information. Distribution and management of such information is not in the scope of the PAWS.

## III. TRUSTED PLATFORM MODULE

Trusted Platform Module (TPM) [13-14] is a low cost and low power security module that a trusted platform relies on for protection. It is typically implemented as an integrated circuit and it can be used as a building block for trusted computing, having other components of the device to rely on it for secure storage read/write and transmission of data. Its architecture is similar to that of a smart card, however it is considered to be fixed and bound to a specific platform rather than being associated with a user. The TPM has several features that make it a useful tool for accomplishing the security goals of the incumbent use registration, device authentication and authorization, and controlling the frequency use.

- Attestation: The TPM attestation mechanism provides the ability for a challenger to verify the state of a platform and which applications are running. Based on this information, a challenger can decide if they wish to consider the platform to be trustworthy or not.
- Secure Storage: The TPM contains a storage root key (SRK) that is stored within the non-volatile memory of the TPM. This key is used as the root of a key hierarchy to access the data being encrypted, and is created during the ownership process along with an owner password (similar to owner authorization). Using the SRK as an encryption key for the data protects it in such a way that it can only be decrypted by using the TPM. All further keys are encrypted and stored outside secure storage. They can be storage keys, binding, or authentication/signature keys. The TPM uses two concepts for data encryption: sealing and binding. Binding is an optional step similar to cryptographic encryption, and it is the operation of encrypting data using a key unique to a specific TPM. Binding can be done outside of the TPM (e.g. remotely) based on a public key of the binding key. However, unbinding must be done within the TPM. Sealing differs from binding as both sealing and unsealing must happen in the TPM. Sealing uses a desired configuration of the platform, and also contains a binding secret known only to the TPM chip. The platform configuration registers (PCR) contain the data for the specific configuration in the volatile memory of the TPM. This means that not only does the same platform have to be used, but it must be in a specific configuration to access the sealed data. This can be used to ensure that no rogue application is running before granting access to the data.
- Ownership: The Opt-in and Ownership mechanisms of the TPM provide accountability and authentication. Ownership must be established in order for all of the TPM features to become available. Before establishing ownership, the user must first opt-in to use the TPM. The TPM has been designed specifically to allow the user to take ownership and configure the TPM. Through the

process of taking ownership, the TPM will transition out of the disabled state and into enabled. When the TPM is enabled, all features can become available.

- Cryptographic Processor: The TPM contains cryptographic tools for generating keys and signatures. This includes a random number generator, SHA-1 engine, RSA Engine, and a key generator.
- Non-Volatile Storage: The non-volatile storage of the TPM contains the Storage Root Key and the Public and Private Endorsement Keys (EK). This is also where Opt-in and Ownership data is stored, as well as program code that is able to run in this shielded location. The TPM provides shielded locations where it is safe to operate on sensitive data such as keys and integrity measurements.
- Volatile Storage: Volatile storage contains the Platform Configuration Registers holding integrity metrics, and Attestation Identity Keys (AIK).

The TPM is a trusted component which the trusted platform relies on for the security foundation of the system. Next sections discuss how the TPM can be used to solve authentication and authorization issues for the white space communications. For regulators responsible for spectrum resources the proposed system will provide tools for enforcing their frequency use related policies.

## IV. Incumbent Protection for TVWS

Incumbent uses in the UHF frequency band are digital TV transmissions and wireless microphones. Here, we focus on the latter as the role of the geolocation database is to protect TV signals. The usage of wireless microphones requires a license from national regulator. In Finland, such authority is FICORA. From FICORA web site it can be seen that in 2012 there were 728 existing radio licenses for wireless microphones. The number of licenses does not indicate the actual amount of microphones as only one license per organization is required. A single organization may have hundreds or even thousands of wireless microphones. The license does not include any information where and when the wireless microphone will be used, nor the information which frequencies are in use. Analyses indicate that there may be up to 60 000 wireless microphones in Finland. It is evident that existing wireless microphone licenses cover only the fraction devices actually in use. This poses a challenge for designing white space system as the information of wireless microphones cannot be obtained from the regulator in many countries. However, there are a few countries that have taken care of this issue already.

One big issue for the low registration activity is the complexity of registration process. To facilitate this, in WISE project [15], management system for wireless microphones has been developed. The system is called PMSE Manager, and it is targeted for all microphone users. Professional users may utilize automatic registration e.g. from Shure Workbench with plug-in, or from Android application for mobile use such as news group reporting from on-site of some event. PMSE

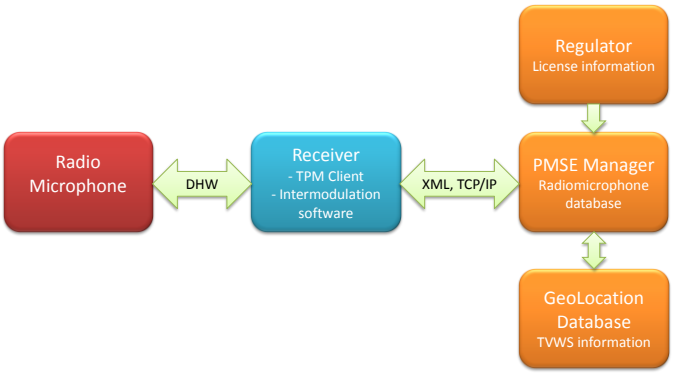


**Figure 1: Overall architecture for PMSE management**

Manager binds licenses from the regulator, the location information of wireless microphone, and utilized frequencies. The system architecture is shown in Fig. 1.

## V. Proposed Architure and Protocol

Assuming that a device would contain a feature for identification, automatic procedure for registration can be defined. Here, we assume that the device contains a TPM chip. We acknowledge that is assumption is not valid for analog and low-end devices. However, in professional set-ups wireless microphones are connected to head-end personal computer, which typically has the Internet access. There, the TPM chip would not cause significant extra cost.

The operational phases of the system are described in Fig 2. When a device is taken into use the first time the binding is formed between the license and the device. Then, after the initial registration, whenever the device is used, the connection is made to PMSE Manager, which performs frequency reservation for the device(s).

The following challenge-response protocol is proposed here to implement registration communication between wireless devices and management server:

- TPM chip in the device produces Attestation Identity Key (AIK), which is a RSA key pair.
- Public key of the device is sent to management server.

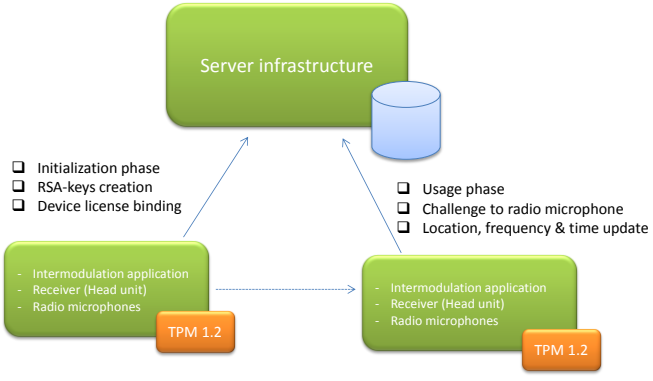


**Figure 2: Two operation modes**

- The server sends a challenge to the device. The challenge is plain text string.
- The device performs the signing of the challenge with the pre-set data from the TPM chip register and the server challenge. The device sends the signed challenge as a response back to the server.
- The server verifies the response with the public key of the device and the original challenge. If the response is valid, the device is added to the server database, and the binding between radio license and the device is formed.

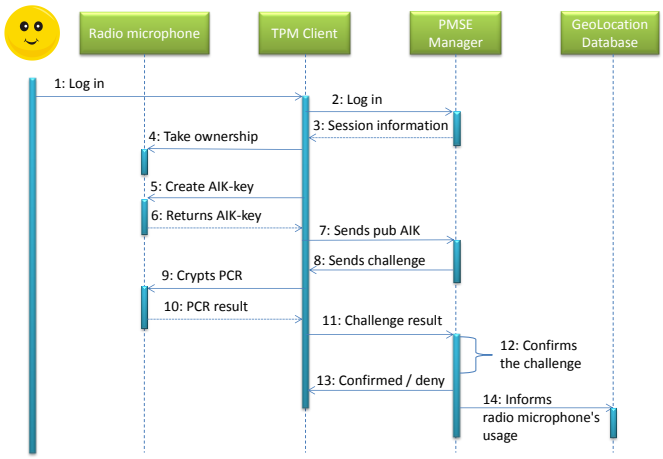


**Figure 3: Sequence diagram for the registration phase**

The operation of the proposed protocol with sequence diagram is illustrated in Fig 3. In Fig 4, the usage phase is shown. There, the PMSE Manager verifies whether the wireless microphone is actually turned on.

As a result for using protocols depicted in Fig. 3 and Fig. 4, automatic and secure device registration has been performed. Also, the utilization of scarce frequency resources is more efficient as utilized frequency is released after the device is offline.

The operation of the proposed architecture has been demonstrated in international seminars such as 30th Wireless World Research Forum (WWRF) meeting in Oulu, April 2013. Source codes from the demonstration have been published as open source at Github [16]. With the source code it is possible to test and verify the proposed architecture.

## VI. Experimental Results

Experimental set-up was built to analyze potential delays in initiating wireless microphone use and releasing frequencies after ending the microphone use. The setup consists of laptop including the TPM chip. This simulates a microphone device. The laptop communicates with the PMSE server, which then negotiates with the geolocation database frequencies to be allocated for microphones. Both the PMSE server and the geolocation database are implemented in Amazon Web Services (AWS). Following tests were run several times to observe possible statistical variation. Results were stable and the effect of data transmission duration was negligible. Table 1. shows operational delays for the enrolling of the microphone, for turning on already registered microphone, and for releasing frequency after the microphone has been turned off.

**Table 1: Experimental operation delays**

| Radiomicrophone turned on and AIK enrollment | |
|---|---|
| Communication protocol phase [16] | Runtime (s) |
| RM_TURN_ON COMM_REQ_CONNECT | 0,002 |
| RM_TURN_ON COMM_PUB_AIK_ENROLLMENT | 0,794 |
| RM_TURN_ON COMM_RSP_CHALLENGE | 0,963 |
| RM_TURN_ON COMM_QUOTE_SUCCESS | 4,667 |
| Total | 6,427 |

| Radiomicrophone turned on (already enrolled) | |
|---|---|
| Communication protocol phase [16] | Runtime (s) |
| RM_TURN_ON COMM_REQ_CONNECT | 0,002 |
| RM_TURN_ON COMM_TURNED_ON | 0,001 |
| RM_TURN_ON COMM_RSP_CHALLENGE | 0,940 |
| RM_TURN_ON COMM_QUOTE_SUCCESS | 4,657 |
| Radiomicrophone total | 5,601 |

| Radiomicrophone turned on, and closed after 10 seconds | | |
|---|---|---|
| Communication protocol phase [16] | Runtime | |
| COMM_REQ_CONNECT | 0,00023 | |
| COMM_TURNED_ON | 0,00049 | |
| COMM_RSP_CHALLENGE | 4,66123 | |
| WAIT NEXT AUTOCHALENGE | 10 | Server is waiting for 10 seconds after microphone has been assigned frequency |
| COMM_AUTOCHALLENGE COMM_REQ_CHALLENGE RM_IS_ON | 0,000771 | |
| COMM_RSP_CHALLENGE | 4,651535 | Here, microphone is still on and no actions are takes |
| Total period time to check microphone status | 14,652306 | |
| WAIT NEXT AUTOCHALENGE | 10 | Server is waiting for 10 seconds |
| COMM_AUTOCHALLENGE COMM_REQ_CHALLENGE RM_IS_OFF | 4,656968 | Microphone has been turned off. Frequency will be released |
| Server reaction time to release the frequency | 14,656968 | |

From the Table 1 it can be seen that with current implementation cryptographic operations take approximately one second and frequency allocation communication between the PMSE server and the geolocation database take over four seconds. It should be noted that both figures are possible to optimize significantly. In the example, the PMSE server waits for 10 seconds between challenges sent to the microphone. This parameter can be adjusted.

## VII. Device Authentication for PAWS Protocol

It is possible to apply procedures from the previous section to authentication of white space devices using the TPM. We take the PAWS protocol as a starting point, and add device authentication on top of it without modifying the existing specification. This part of the paper is regarded as a work in progress, since the PAWS specification has not been finalized.

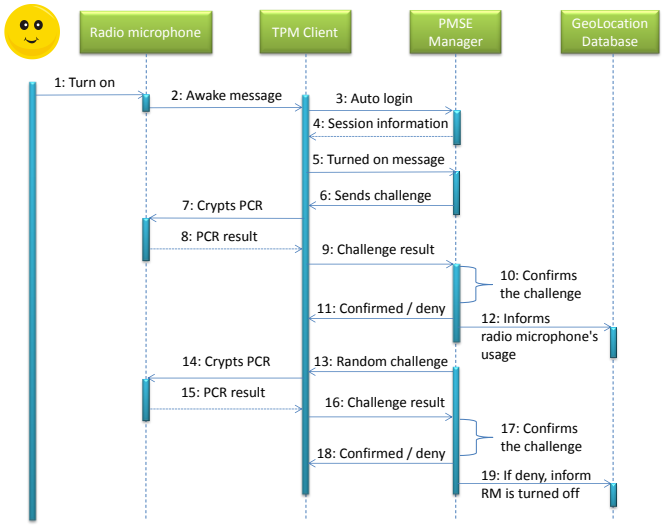


**Figure 4: Sequence diagram for the usage phase**

Procedures from the section V are adapted as follows: During WSD authentication, the device sends the public key of AIK to the geolocation database, which responses with a challenge the WSD. Then the WSD sends unique cryptographic

response to the geolocation database, which confirms the challenge response.

A TPM EK and AIK need to be related to publicly verifiable certificate. The AIK certificate needs to be verified by the entity receiving public AIK. The authentication system implements a service for this functionality. The service is called a Certificate repository. It is a global server, which contains all TPM RSA key certificates for white space devices. The information is populated by device manufacturers.

The purpose of certificate repository is to have a server acting as a trusted third party, which signs and validates RSA keys from the TPM. This will form a triangle system (see Fig. 5), where the mutual authentication between the device and the geolocation database can be performed.

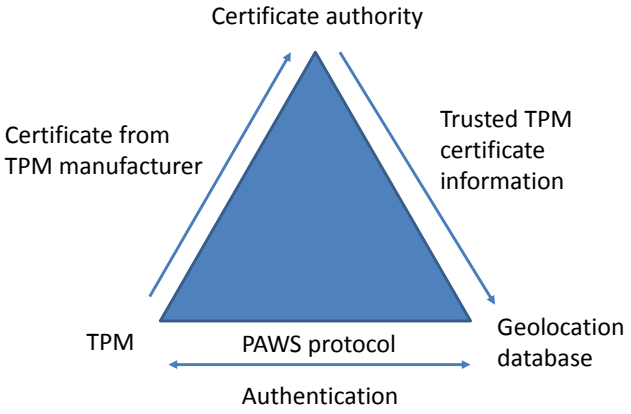


**Figure 5: Authentication model for white space devices**

## VIII. CONCLUSIONS

Long term research topic – dynamic spectrum utilization is becoming commercial as standardization and regulation is going forward globally. TV white space technology implementation is the first step in the direction of collective spectrum use.

In this paper, device authentication for TV white space system was discussed. The system is based on the TPM. The first use case was the automatic registration of wireless microphones. For this case, open source implementation and demonstration is available from [16]. Experimental results show indicative delays due to the authentication protocol.

Similar procedure was also applied to authentication of white space devices using PAWS protocol. The proposed method increases spectrum efficiency, in addition to increased security and reliability, due to the usage monitoring capability.

Similar architecture may be utilized also for other dynamic spectrum access systems, which are controlled by central database.

## ACKNOWLEDGMENT

The work for this paper has been performed in ReWISE project funded by Tekes – the Finnish Funding Agency for Innovation. The results in this paper are obtained with close collaboration with project partners University of Ontario Institute of Technology (UOIT), Fairspectrum, Nokia, and Finnish Communications Regulatory Authority (FICORA).

## REFERENCES

[1] RSPG, "Report on Collective Use of Spectrum (CUS) and other spectrum sharing approaches", RSPG11-392, European Commission, Radio Spectrum Policy Group, Nov. 2011.

[2] M. Cave and W. Webb, "The Unfinished History of Usage Rights for Spectrum", *Proc.* 2011 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Aachen, Germany, May 2011.

[3] CEPT, "Technical and operational requirements for the possible operation of cognitive radio systems in the 'White Spaces' of the frequency band 470-790 MHz", ECC Report 159, Jan. 2011.

[4] H. Karimi, "Geolocation databases for white space devices in the UHF TV bands: Specification of maximum permitted emission levels", *Proc.* 2011 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Aachen, Germany, May 2011.

[5] R. Murty, R. Chandra, T. Moscibroda and P. Bahl, "Sense*Less*: A Database-Driven White Spaces Network", *Proc.* 2011 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Aachen, Germany, May 2011.

[6] S. Arkoulis, L. Kazatzopoulos, C. Delakouridis and G.F. Marias, "Cognitive Spectrum and its Security Issues", *Proc.* The Second International Conference on Next Generation Mobile Applications, Services, and Technologies (NGMAST 2008), Cardiff, Wales, 2008.

[7] T. Brown and A. Sethi, "Potential Cognitive Radio Denial-of-Service Vulnerabilities and Protection Countermeasures: A Multi-dimensional Analysis and Assessment", *Proc.* 2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2007), Orlando, USA, 2007.

[8] Z. Chaczko, R. Wickramasooriya, R. Klempous and J. Nikodem, "Security Threats in Cognitive Radio Applications", *Proc.* 14th International Conference on Intelligent Engineering Systems (INES 2010), Canary Islands, Spain, 2010.

[9] S. Chen, K. Zeng and P. Mohapatra, "Hearing is Believing: Detecting Mobile Primary User Emulation Attack in White Space", *Proc.* The 30th IEEE International Conference on Computer Communications (IEEE INFOCOM 2011), Shanghai, China, 2011.

[10] T.R. Newman, T.C. Clancy, M. McHenry and J.H. Reed, "Case Study: Security Analysis of a Dynamic Spectrum Access Radio System", *Proc.* IEEE Global Communications Conference 2010 (GLOBECOM 2010), Miami, USA, 2010.

[11] PAWS protocol, https://datatracker.ietf.org/wg/paws/

[12] RFC 6953, https://datatracker.ietf.org/doc/rfc6953/

[13] Trusted Platform Module, http://www.trustedcomputinggroup.org/developers/trusted_platform_module.

[14] Trusted computing group, "TPM Main Part 1 - Design Principles", Available on-line: http://www.trustedcomputinggroup.org/files/static_page_files/72C26AB5-1A4B-B294-D002BC0B8C062FF6/TPM%20Main-Part%201%20Design%20Principles_v1.2_rev116_01032011.pdf.

[15] WISE project, http://wise.turkuamk.fi/

[16] https://github.com/WISEProject/TPM-implementation-for-device-authentication