On Database for Mobile Phones Ownership

Dmitry Namiot
Lomonosov Moscow State University
Moscow, Russia
dnamiot@gmail.com

Manfred Sneps-Sneppe
ZNIIS
Moscow, Russia
manfreds.sneps@gmail.com

Abstract—**This article examines the confirmation of mobile phone ownership. We propose a model of digital certificates that can be used to programmatically check the lawful use of the device. The developed model combines device identification and proper identification of the owner in social networks. As a practical deployment and use cases we discuss an additional check for authorization of mobile users in various services (for example, financial applications).**

I. INTRODUCTION

In the telecommunications industry a service provider can record information regarding a mobile communication device at the time of activation of service [1]. For example, each communications device's International Mobile Equipment Identity (IMEI) contains information regarding that device. This information tells telecom provider what type of device is being used. It lets telecom operator know what functionality is available on that particular device. In the same time mobile device has got a removable Subscriber Identity Module (SIM) card. SIM cards are gradually replaced by UICC (Universal IC Card), starting from 3G. SIM card contains information related to the mobile user (subscriber) and allows the device to work with the particular mobile network. The information on the SIM card (part of it) is transmitted each time a user connects to a network. Technically, telecom provider can know the relationship between the SIM card and the IMEI. For example, this information could be collected at the time of SIM card activation. SIM cards distribution is subject to regulation (e.g., it is so in Russia). So, the telecom provider knows the person behind the particular SIM card. As soon as we have a link SIM -> IMEI, we can discover the owner of particular phone. On practice, telecom operator is the only owner of this information (at least, potentially).

In the same time, a user may transfer the SIM card from one device to another without the telecom operator ever learning of the switch. In the past, home location register (the main database at the telecom operator) contained mobile identification number. It was needed in order for mobile device to be used. And subscribers were unable to make changes to their equipment without involving the telecom operator. The modern approach gives the more freedom to the users, but creates the problem for operator in providing the optimal service (the actual device is unknown). We can mention also security issues as a result for SIM card portability. For example, a stolen or lost mobile device may be used by anyone with an active SIM card by simply replacing the SIM card into the stolen or lost phone.

It means that telecom provider theoretically should track SIM cards data in conjunction with IMEI. Of course, it should be performed in the real time, what could be an additional technical problem. This information can be used in many ways. For example, by matching SIM data with IMEI data, telecom operator may determine that a device that has been reported lost or stolen is being used. Operator may track and locate the device in question or even disable the service for that particular device. Yes, the information about the device could be used in services to align capabilities for both parties, but in this paper we will discuss lost and stolen devices. So, the ideal picture is presented on the Fig. 1.

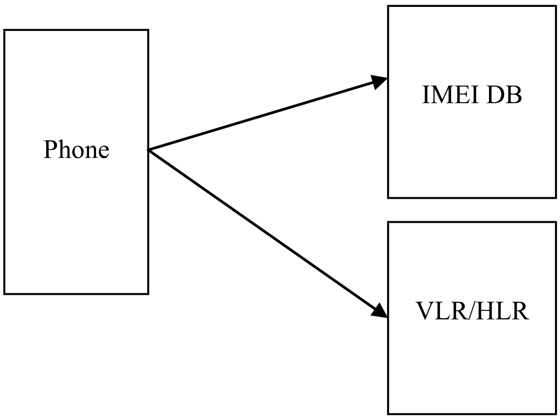


Fig. 1. IMEI DB & HLR

The question is how to present this picture for non-operators environment? Can we do that without the SIM card? The main reason for this switch is to present open Application Program Interfaces to this ownership information. But telecoms are not very willing to provide open interfaces to their data.

The rest of the paper is organized as follows. The Section II describes approaches to mobile phones identification and discusses the related works. The Section

III describes our social digital certificates for ownership. And the Section IV discusses some use cases and practical applications.

II. Mobile phones identification

There are several factors that could be used for the identification.

International Mobile Subscriber Identity (IMSI) number. It is a unique number associated with all GSM and Universal Mobile Telecommunications System (UMTS) network mobile phone users. It is stored in the SIM card. An IMSI is usually 15 digits long. The first 3 digits are the Mobile Country Code, and are followed by the Mobile Network Code (MNC). The remaining digits are the mobile subscriber identification number (MSIN) within the network's customer base. This number will also be stored in the server's database for each client.

IMEI is a unique 15 digits number assigned to an individual device. IMEI can be used to determine information associated with the device. This information includes the manufacturer and model type. An associated parameter for the IMEISV (International Mobile station Equipment Identity and Software Version number) is 16 digits number.

The IMEI includes a Type Allocation Code (TAC) of 8 decimal digits and the Serial Number (SNR) of 6 decimal digits plus a Spare decimal digit. The TAC identifies the type of the Mobile Equipment and is chosen from a range of values allocated to the Mobile Equipment manufacturer in order to uniquely identify the model of the Mobile Equipment. The SNR is an individual serial number that uniquely identifies each Mobile Equipment within the TAC. The Spare digit is used as a check digit to validate the IMEI and is always set to the value 0 when transmitted by the Mobile Equipment [2].

The IMEISV is 16 decimal digits long and includes the TAC and SNR same as for the IMEI but also a 2 decimal digit Software Version Number (SVN) which is allocated by the Mobile Equipment manufacturer to identify the software version of the Mobile Equipment [2].

Mobile operating system APIs provide applications with large amounts of information about users. Applications can query mobile APIs for the user's location, list of contacts, browser and download history, list of installed applications, and IMEI [3]. Consumer IMEIs have value to black market phone vendors. When a phone is reported stolen, its IMEI is blacklisted. Theoretically (it depends on telecom operator) this black listed database could prevent mobile phone from connecting to the network. It could make stolen phones useless. In practice, thieves can alter phone IMEIs to replace blacklisted IMEIs with valid IMEIs [4].

To address IMEI theft, mobile operating systems could provide applications with an alternate, globally-unique device ID [3]. E.g., [5] suggests the obvious method to do this is to compare the internally stored IMEI with the IMEI printed on the phone (commonly located under the battery). In other words, it is also highlights the need for some external database, where IMEI is just a part of data.

In the same time studies for mobile communities show that only a very small percentage of the participants (less than 24%) knows his/her phone's IMEI [6]. Almost half of respondents are completely unaware of its existence [7].

IMEI is very often used a part of Multi Factor Authentication with mobile phone [8]. Multi factor authentication refers to the use of more than one factor in the authentication process [9]. One form of attack on networked computing systems is eavesdropping on network connections to obtain authentication information. For examples third party can obtain the login ID and password of legitimate user. Once captured, this information can be used at a later time to gain access to the system. One-time password (OTP) systems are designed to counter this type of attack [10]. An OTP is valid for only one login session or transaction. OTPs prevent a number of shortcomings associated with traditional authentication (such as user names and passwords) [11]. IMEI is usually a part of OTP calculation.

For example, during the registration phase, users are compelled to use their personal information (username, password, PIN, etc.) in addition to the IMEI. As the next step, we can perform an IMEI validation check for the mobile phone of the user. We can prevent from registering in the system users with not valid IMEI. Thus, the user is compelled to enter a valid IMEI during registration [12]. Alternatively, what is important for our issue, we can collect that IMEI from some external database.

In addition, we can check if the IMEI and the mobile number are repeated. It means that it is registered by another user, so we can stop the registration process. The use of this method ensures that every user has one mobile number and one IMEI number.

In our paper we propose some external database with IMEI numbers that could be used in registration processes as a confirmation for phone ownership.

III. Digital certificates

The main goal for research is some external database that could be used for mobile phone ownership confirmation. By our vision this database should be disconnected from telecom operators (see Fig. 1.). The main reason for this disconnection is the need for open API for this database. Traditionally, telecom operators are weak in presenting access to own data. So, independently hosted and maintained data store could be more developers friendly. The project itself was developed as Open Source software in university. The project itself could be community maintained entity. Also we offered this software to ZNIIS institute, who maintains mobile number portability database in Russia.

Of course, filling this database of ownerships must be completely voluntary. As per some analogy: the owner of a dog that places the badge with own coordinates (e.g. mobile phone) on her collar.

So, there are two main questions:

- how to identify a phone,
- how to identify an owner.

As per phone identification we will use the above mentioned IMEI. It means that as a mechanism for identification we should use some mobile application. Mobile application (e.g. Android app) has got access to IMEI, so it could be read and saved somewhere.

Public class *TelephonyManager* (*android.telephony.TelephonyManager*) provides access to information about the telephony services on the device. Applications can use the methods in this class to determine telephony services and states, as well as to access some types of subscriber information. Applications can also register a listener [13] to receive notification of telephony state changes.

Public method *String getDeviceId ()* returns the unique device ID, for example, the IMEI for GSM and the MEID or ESN for CDMA phones. It returns null if device ID is not available.

Now let us talk about owner's identity. Nowadays, most (if not all) mobile users are members of some social networks. Our idea is to use social identity as a confirmation of phone ownership.

In social networks users can build profiles for storing and sharing various types of content with others. And what is interesting for us, social-networking sites expose their networks to Web services in the form of online application programming interfaces. These APIs allow third-party developers to interface with the social-networking site, access information and media posted with user profiles [14]. Social networks provide numerous application services that can mash up user-profile data with third-party data. As it is mentioned in [14], all major social networks have begun launching social-networks connect services such as Facebook Platform, Google Friend Connect, etc. These services break down the garden walls of social-networking sites and let third-party sites develop social applications and extend their services without having to either host or build their own social network. This extension allows third-party sites to leverage the social-networking site's features. What is especially interesting for us, third-party sites can exploit the authentication services provided by a social-networking site so that users need not create another username and password to access the third-party site. Instead those, users can rely on their social-network credentials and established profile. Alternatively, the third-party site can obtain users' profiles from the social-networking site to create an enhanced experience.

This brings us to the idea of digital certificates: IMEI, confirmed by (signed with) social networks ID. It eliminates the need for yet another user name/password database and, what is very important also, it eliminates the need for saving users' personal data. Our digital certificate contains IMEI and a link to the profile in social network. So, in this schema we rely on data in social network. There is no need to copy personal data to some external location. So, each certificate is just a pair: (IMEI, Social ID).

Social ID has got a form of link to user's profile. E.g. *http://facebook.com/user_name.*

Let us see Facebook Connect (Fig. 2). Facebook Platform contains several APIs:

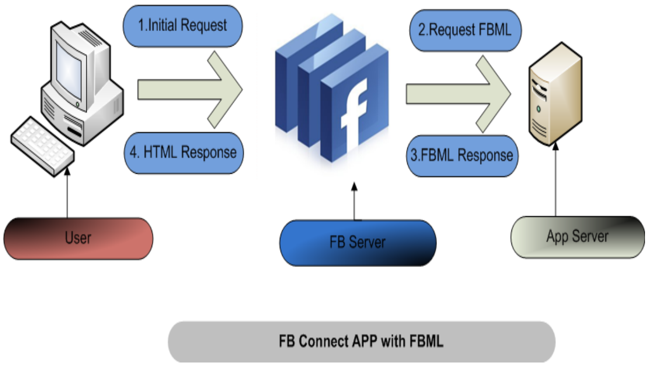


Fig. 2. Facebook Connect

Identity authentication. It proves users' identity. So, users can authenticate using their existing accounts from Facebook.

Authorization governs access to user data in Facebook based on predefined authorization access rights. This authorization API lets third-party sites create new content and extract existing content from users' data in Facebook.

Streams let third-party sites publish to users' activity streams and vice versa.

Applications let third-party sites develop rich social features in the form of applications and thereby extend Facebook.

Authentication is, probably, the most used component from Facebook Platform. This API enables third-party sites to leverage Facebook as an identity provider. Users can use their existing Facebook profile to authenticate. Facebook leverages OAuth 2.0 [15] for authentication and authorization. OAuth 2.0 is a simplified, improved version of the Open Authorization standard that lets third-party sites obtain authorization tokens from Facebook. First, a user of the third-party site authenticates using Facebook as an identity provider. Next, Facebook issues a token that lets the third-party site access the user's basic profile information.

The typical examples of Facebook Connect usage are customized check-ins [16].

In our case digital certificates suite includes a mobile application (currently – it is for Android). This mobile application incorporates Facebook Connect library for Android. Application reads IMEI, asks users to authenticate using Facebook and create a new certificate. There is no need in obtaining additional permissions; successful authentication is used just for creating a proper URL to Facebook profile. Usually, this URL has got the following form:

http://facesbook.com/UserID.

Where *user_name* is just an alias for this ID.

As soon as the certificate is calculated, we can store it in some external database. So, the above mentioned telecom-related picture (Fig. 1) is transformed to this:

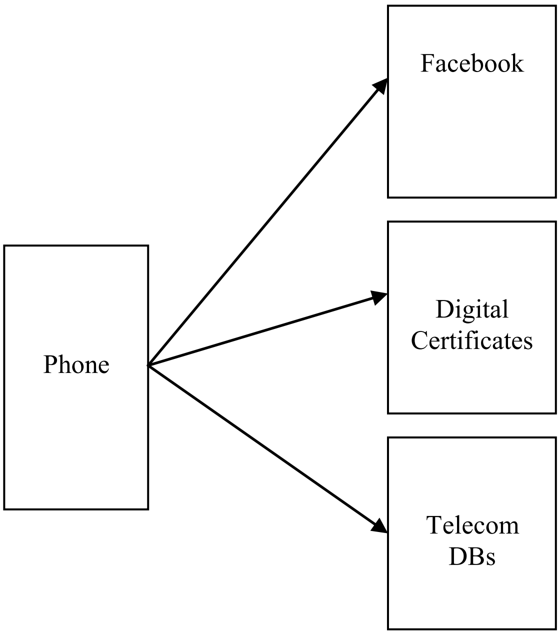


Fig. 3. Digital Certificates

So, our platform for digital certificates contains the following components:

- Mobile application for creating certificates.
- Web-hosted database with certificates.
- Web-based UI for access to database (e.g., perform a search).
- API for programmable access to database (e.g., perform a search from applications).

Finally, the whole picture is very straightforward. Mobile user (owner of the phone) can voluntarily create a digital certificate for own phone. This certificate is an identification number (IMEI), signed by referring to the user profile in a social network (Fig. 4).

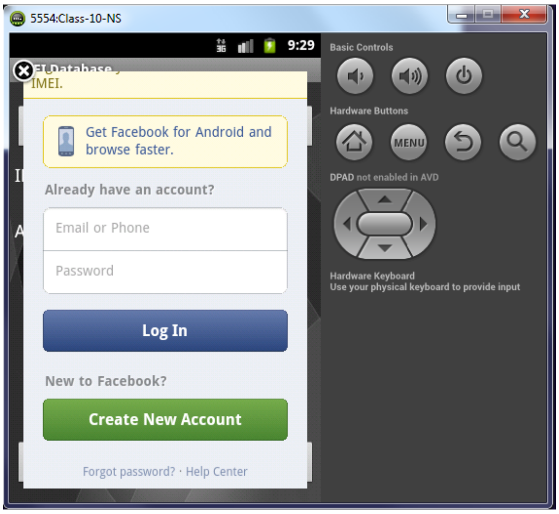
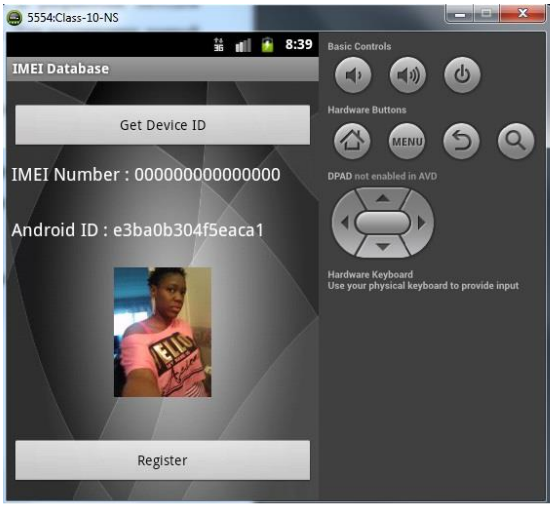


Fig. 4. Facebook authentication

In the current implementation we used Facebook as a social network. But technically it could be any network with open API for authentication. Of course, the user must use this application only once. As soon as certificate is created, it is saved in public available database (Fig. 5).



IMEI Number : 000000000000000

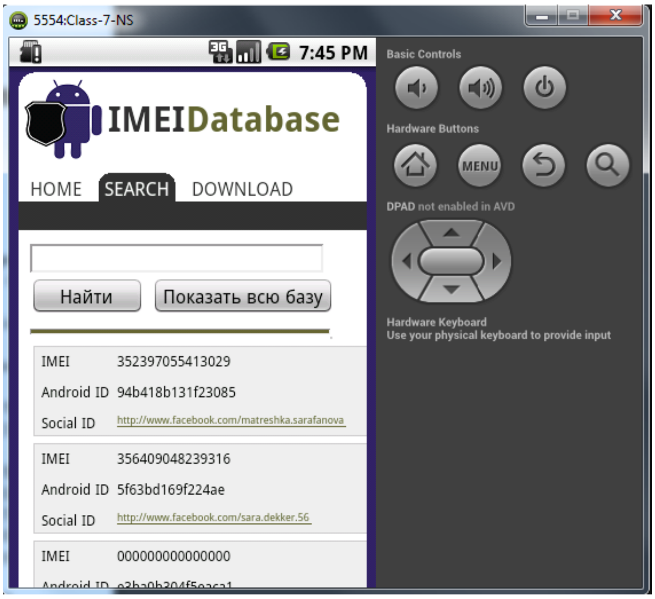
Android ID : e3ba0b304f5eaca1

Fig 5. Digital certificate

As soon as this database if publicly available, the process of checking the phone owner is greatly simplified. Web-based UI allows DB search by IMEI and/or by social ID. And this, in turn, is able to stop some significant percentage of mobile subscribers from using the phone, which came to him not quite a legitimate way. Moreover, such a framework could be help for the official investigation.

Database for certificates lets users only add records. So, for the each phone it will keep timestamped list of certificates. So, any current owner of the phone can add a new record with own identification. But he cannot change the previously collected information. Of course, he can see it but cannot edit or delete. And this mechanism allows to re-sign IMEI with other social network ID.

The usage of social network (Facebook in this case) lets us eliminate the need for saving personal data in this database. It is very important from the practical point of view, because storing personal data could be a subject for a special regulation in some countries. In our case database keeps only a link (public link) to the social network profile without any personal details (Fig. 6).



IMEI 352397055413029
Android ID 94b418b131f23085
Social ID http://www.facebook.com/matreshka.sarafanova

IMEI 356409048239316
Android ID 5f63bd169f224ae
Social ID http://www.facebook.com/sara.dekker.56

IMEI 000000000000000
Android ID e2ba0b304f5eaca1

Fig. 6. Search database

As side result database provides actually some form of the social networks (social circles) inside of Facebook. Each such circle contains a list of all owners for the particular phone.

Thus, the general idea of this model is not in tracking lost (stolen) phone. Certificates introduce the possibility of checking the phone's owner at the time of using the phone. In this case, first of all, we mean the use of smart phones on the Internet. The idea is that for many mobile application users will use the same Facebook Connect for authentication. And authentication module for mobile application is mobile application too. So, this third party application can obtain IMEI, perform a search in database for digital certificates, obtain a social ID and compare it with ID, just provided by the mobile user. It is the simplest use case: application during user's authentication via social network can check out who owns this phone. Of course, it is completely up to application what to do with this information. For example, it can send a warning (alert) to user's email about access from new device or even prevent the access unless user confirm it, etc.

Technically, nothing prevents operators from using the same open database to verify the owners at the time of making calls and sending SMS.

Users can search database via mobile application and web (including mobile web).

Digital Certificates is Open Source application [17]. Web part developed on PHP, data store uses MySQL database.

The term *Digital Certificates* has been selected by the analogue with crypto algorithms. Actually, this idea for linking social profiles with some hardware identification could be extended beyond the phone.

IV. USE CASES

Web link for search could be QR-coded and printed on the sticker. So, we will get a physical form for digital certificate. QR-code contains URL for search particular IMEI. It could be some analogue for context-aware QR-code [18].

The next possible direction is programming API for digital certificates data base. Technically, it is REST based HTTP interface. It lets obtain ownership info (get chain of records) programmatically. For example, applications similar to Geo Messages [19] or WATN [20] will be able to check identity rights of sender.

Checking ownership for mobile phone could be useful for finance applications, for example. Application could be aware of social ID for mobile users or it can offer the same Facebook login for authentication. In both cases application can compare this ID with ID that corresponds to the current IMEI in database of digital certificates. Here is the basic example for Facebook login:

```
  FB.login(function(response) {

     if (response.authResponse) {

       console.log('Welcome!  Fetching
your information.... ');

       FB.api('/me', function(response)
{

         console.log('Good to see you, '
+ response.name + '.');

  // here we can add code for IDs
comparison

       });
```

```
      } else {
        console.log('User cancelled login
or did not fully authorize.');
      }
   });
```

Such kind of authentication with additional checking could be a useful add-on for the customized check-in systems [21, 22] or local messaging applications [23]. In both cases we add an additional level for users' identity checking.

Actually, the link between phone identity and social identity is probably used by Google for preventing unauthorized access to Gmail on Android. It could be one of the many elements for checking user's identity. Database for digital certificates with public API opens this possibility for all applications.

V. Conclusion

In this paper we propose digital certificates for phone ownership. Each certificate combines phone identity (IMEI) and social ID. It lets check phone ownership via web search (including mobile web), mobile application or via API. In general, our digital certificates can add an additional checking layer for mobile authentication. The proposed approach has been implemented as Open Source project.

Acknowledgment

We would like to thank A.Kolosova for an initial release of digital certificates in her diploma at Lomonosov Moscow State University (supervised by D. Namiot) [24].

References

[1] Cardina, Donald M., and Anastasios L. Kefalas. "System and method for IMEI detection and alerting." *U.S. Patent* No. 8,126,432. 28 Feb. 2012.

[2] Gosden, Paul, et al. "A Uniform Resource Name Namespace for the GSM Association (GSMA) and the International Mobile station Equipment Identity (IMEI)." (2013).

[3] Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011, October). A survey of mobile malware in the wild. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (pp. 3-14). ACM.

[4] iClaried. How to change your iPhone IMEI with ZiPhone (Windows). http://www.iClarified.com/entry/index.php?enid=657

[5] Willassen, S. (2003). Forensics and the GSM mobile telephone system. International Journal of Digital Evidence, 2(1), 1-17.

[6] Androulidakis, I., & Kandus, G. (2011, April). Mobile Phone Security Awareness and Practices of Students in Budapest. In ICDT 2011, *The Sixth International Conference on Digital Telecommunications* (pp. 18-24).

[7] ITwire, "One-third of Aussies lose mobile phones: survey", ITwire article, http://www.itwire.com, 2010 [accessed: 16/12/2013]

[8] Aloul, Fadi, Syed Zahidi, and Wasim El-Hajj. "Multi Factor Authentication Using Mobile Phones." *International Journal of Mathematics and Computer Science 4* (2009): 65-80.

[9] Jing-Chiou Liou and S. Bhashyam, A feasible and cost effective two-factor authentica tion for online transactions in International Conference on Software Engineering an d Data Mining (SEDM), 2010. pp. 47-51, IEEE.

[10] Jongpil Jeong, Min Young Chung, and Hyunseung Choo. Integrated OTP-based User Authentication Scheme Using Smart Cards in Home Net works. Proceedings of the 41st Annual Hawaii International Conference on System Sciences. 2008. Waikoloa, IEEE.

[11] K.Aravindhan and R.R.Karthiga, One Time Password: A Survey. *International Journal of Emerging Trends in Engineering and Development,* 2013. 1 (3): p. 613-623

[12] Hussein, K. W., Sani, N. F. M., Mahmod, R., & Abdullah, M. T. (2013). A Novel Authentication Scheme to Increase Security for Non-Repudiation of Users.

[13] Android SDK Reference http://developer.android.com/reference/android/telephony/TelephonyManager.html#getDeviceId%28%29 Retrieved: Feb, 2014

[14] Ko, M. N., Cheek, G. P., Shehab, M., & Sandhu, R. (2010). *Social-networks connect services. Computer*, 43(8), 37-43.

[15] Hardt, Dick. "The OAuth 2.0 Authorization Framework." (2012).

[16] Namiot, D., & Sneps-Sneppe, M. (2011). Customized check-in procedures. In Smart Spaces and Next Generation Wired/Wireless Networking (pp. 160-164). Springer Berlin Heidelberg.

[17] Digital Certificates http://fr30706.tw1.ru/ Retrieved: Feb, 2014

[18] Namiot, Dmitry, Manfred Sneps-Sneppe, and Oleg Skokov. "Context-aware QR-codes." // World Applied Sciences Journal. — 2013. — Vol. 25, no. 4. — pp. 554–560 DOI: 10.5829/idosi.wasj.2013.25.04.11360

[19] Namiot, D. "Geo messages", In Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 *International Congress* on (pp. 14-19). IEEE. DOI: 10.1109/ICUMT.2010.5676665

[20] Dmitry Namiot and Manfred Sneps-Sneppe. "Where Are They Now–Safe Location Sharing." Internet of Things, Smart Spaces, and Next Generation Networking. Springer Berlin Heidelberg, 2012. 63-74. DOI: 10.1007/978-3-642-32686-8_6

[21] Namiot, D., & Sneps-Sneppe, M. (2011, October). A new approach to advertising in social networks-business-centric check-ins. In Intelligence in Next Generation Networks (ICIN), 2011 *15th International Conference on (pp. 92-96). IEEE.*

[22] Namiot, D., & Sneps-Sneppe, M. (2013, March). Wireless Networks Sensors and Social Streams. In Advanced Information Networking and Applications Workshops (WAINA), 2013 27th *International Conference on (pp. 413-418). IEEE.*

[23] Dmitry Namiot and Manfred Sneps-Sneppe. "Local messages for smartphones". Future Internet Communications (CFIC), 2013 *Conference on (pp. 1-6). IEEE.* DOI: 10.1109/CFIC.2013.6566322.

[24] Namiot, D.E., & Kolosova, A.I. (2013). Checking of mobile phone owner. *International Journal of Open Information Technologies*, 1(8), 26-31. (in Russian)