

The information system for enterprise visitors' verification, identification and authentication utilizing modern identification features

A Y Iskhakov¹, R V Meshcheryakov¹

¹ Tomsk State University of Control Systems and Radioelectronics, 40, Lenina Ave., Tomsk, 634050, Russia

E-mail: iaiy@security.tomsk.ru

Abstract. The problem of distant enterprise visitors' verification, identification and authentication in case of the pass regime is investigated. In order to solve the problem, a structure of the information system utilizing modern identification features is suggested. The article presents the access control systems identifiers classification and an overview of modern identification features and data transmission technologies.

1. Introduction

Lately, the access control system (ACS) has been one of the most effective methods to solve the problem of complex security of the different property objects [1]. ACS allows preventing nonauthorized (illegal) access to the object territory, into the building or some floors. At the same time, the systems of such a kind do not prevent the staff and visitors from entering the allowed areas. ACSs are installed at the objects of different kinds: ranging from small offices to big plants and technoparks with several buildings. Wide application of such systems leads to the fast development of technologies used.

One of the problems solved with ACS is identification of every visitor (the subject of access) and the subsequent opportunity to enter the allowed areas [2]. This procedure utilises comparison of the identification features attached to some particular subject with the data base information. When the members of the staff is it concerned there are used contact or contactless cards [3] of different forms and standards. Table 1 shows the classification of the modern access identifiers.

There are many enterprises which functional peculiarities need a path regime with the opportunity for outside people to visit them. The goal of such visits could be excursions, exhibitions, scientific and practical seminars [4]. Individual electronic passes for the outside people are expensive, therefore the most popular way of the visitors identification is inspection of the document certifying the person followed by registration in the registry. This way is not effective, because identification is done only at the entrances controlled by the security staff. In addition, the policy of total inspection is not effective, because it slows the business process.

The alternative way to solve the problem is the on-line service when the visitor can order the pass to the object himself. After registration, the visitor would receive the one-time pass with a bar code, print it himself and use at the electronic equipped entrance. But in this case, it is impossible to identify the visitor personality, impossible to check the validity of the data written by the visitor. Besides, such



method does not allow one to check legitimacy of the identifier, in other words, does not allow identifying the visitor. Thus, the information system with the following functions becomes actual:

- An opportunity of the distant registration of the visitor without preliminary visit.
- Verification of the visitor personality at the stage of registration.
- A possibility to use modern identifications.
- Realization of the authentication procedures.
- An opportunity to install the system into modern ACS.

In order to realize these functions, it is necessary to define the procedures for the following stages: registration, identification and authentication of the visitor.

Table 1. Classification of the modern ACS identifiers

Identification features used	Basic element for use	Examples of identifier	Examples of reading devices
Mechanic	Elements of the identifier construction	Mechanical keys with perforating holes	Abloy SL905, Mottura 54.793
Magnetic	Magnetized parts of the surface or magnetic identifier elements	Cards with magnetic strips, Wiegand cards	Cipher MSR210U-33, Posiflex MR-2106U
Optic	Marks put on the surface or inside identifier having different optical characteristics in case of the reflected or transmitted illumination	Cards with a bar code, topographical labels	AP-IRC, CBH-4_KMKS
Electronic contacts	Electronic code written into the identifier microchip	Electronic keys	ACR38U-I1, OMNIKEY® 3121
Electronic radiofrequency	Radio channel used to transmit the data	Contactless cards of excess	Bolid PROXY-3A, Matrix II IronLogic
Acoustic	Coded acoustic signal	Device to generate acoustic signals	Stelberry M-70, Invensense NMP621
Biometric	Individual person physical features	Fingerprints, palm geometry, voice, signature dynamics	Smartec ST-FR030EMW, BioSmart PV-TS
Combination	Several identification features	Contactless access card and fingerprints	Smartec ST-FR031EM, ACR83

2. Registration and verification of the visitors

To realize the distant registration of a person, it is suggested to work out the system utilizing web-oriented architecture not needed addition soft at the visitor side. The traditional scheme of a visitor registration in ACS is shown in Fig. 1.

The distant verification of a registered person includes delegation of the mechanism M2 authority to mechanism M1. To do this, the author suggests using the framework based on the mechanism of trusted persons in the ACS registration sub-system. In this case, other people who previously controlled the legacy of the operation and also have needed privilege should affirm the personality of the visitor. The John Branard group was the first to suggest this mechanism. They realised and tested the system utilizing the social authentication when the visitor personality was proved by other people.

The successful example of this system application is working up to the present system of renovation of access to the account «Trusted Contacts», used in the social network, Facebook, since 2013. A visitor can name several friends to prove his personality using a special key in case the

account is blocked. It is considered that these people can telephone the visitor or meet him personally to prove the legality of the access restoration. The administration of the social network thinks that this way is safe, secure safe and secure for the access restoration. In case of Facebook, the mechanism of trusted people is applied to restore the access to the existing accounts. The author is going to apply the method for personality verification before the account is written.

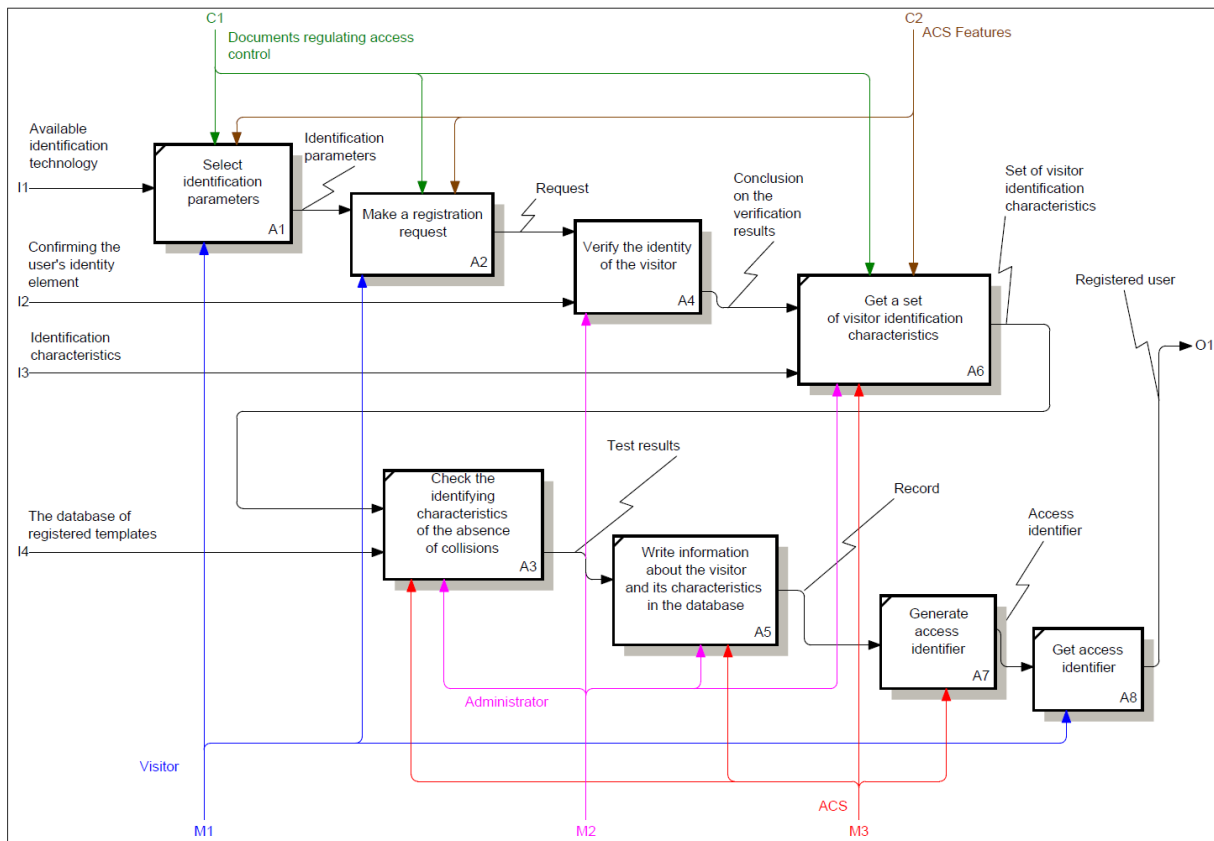


Figure 1. The traditional scheme of an ACS user registration

3. Identification and authentication

3.1 The modern identification features

According to statistics, presented by the International Telecommunication Union by 2016, there were used 7 377 million of mobile communication devices (the population of the Earth is about 7 448 million). A cellular telephone came into the everyday life and one cannot imagine life without it. So, the author suggests integrating the fast developing mobile technology into the industry of security to use the mobile device (smartphone) as the access identifier.

The modern smartphones, having powerful calculating opportunities, large memory and fast access to the Internet can not only provide mobile communication, but at the same time also keep several virtual passes allowing access to different objects with the help of a telephone [5]. Further, the main advantages of the method compared to electronic passes are given.

Advantages of application

- There is no need to use several identifiers (electronic passes) - each for every object.
- An opportunity of operational distant identification control including issue, change and recall.
- An opportunity of hidden reading devices (RD) installation (not entering the room), vandalism protection.
- An opportunity to use in case of longer distances (as an example, a barrier at the entrance of the parking place or the garage).

Security

- Mobile operation systems controlling the modern smartphones provide reliable security. In addition to the OS security service, it is also possible to use devices of electronic signature and coding. Besides, mobile applications work within the isolated program area (Sandbox) without the possibility of access and data variation by other programs.
- Basic functions of a screen automatic blocking with the demand of several passwords provide an opportunity to put in the additional authentication factor.
- Modern telephones allow using a functional that would inform the owner about the device position in case it is lost.
- A probability to find the lost telephone is much higher than the access with the card.
- The probability to transfer the smartphone to other people is lower than in case of the access card.

Convergence opportunities

A mobile communication device used for identification can be also used to restrict the access to the physical objects and to the organization electronic resources. The following examples can be mentioned: authentication of the means of wireless communication, VPN, corporative portals and others.

3.2 Data transmission technology

Among different technologies of data transmission used in mobile devices, Near field communication (NFC), Bluetooth Smart (BLE) and processing the coded information on the smartphone screen are most convenient for the identification of data transmission in ACS [6].

NFC is a technology of wireless high frequency communication for not large distances having three modes:

- passive (emulation of a smart-card). A passive device works as a contactless card of one of the standards;
- data transmission by the devices equal in rights;
- an active mode (reading or writing).

In order to emulate access with the mobile device, it is necessary to have the Secure Element (SE), a SIM-card for example. For the centralized SE, an ecosystem using the Trusted Service Manager (TSM) was worked out. This leads to the complicated technical processes of integration and to business models making application of contactless NFC more difficult [7]. In 2013, the Google company introduced the technology of Host-Based Card Emulation into operational system Android (HCE), allowing the emulation of the contactless card into the mobile application without SE. The drawback limiting the application of NFC technology is absence of its support in some mobile OS dissimilar Android.

The technology of Bluetooth Smart (BLE), presented in 2010, allows transmitting data between the devices at the distance of several tens of meters, having low energy consumption and needing no compulsory procedures of the devices conjugation (compared to mating Bluetooth). BLE is the only contactless technology which is supported by many mobile OSs. The obvious advantage of the technology of a larger radius adds some drawbacks and needs additional protection of the transmitted identity data.

Displays of the modern smartphones have rather good resolution, allowing one to use them to show the data on the screen. So, the reading device should be a video camera which signals are processed by the access controller. For transmitting the identity data, it is better to use the barcode coding algorithms. One of the examples is the OR-codes technology having a big volume of the transmitted information and a high speed of recognition [8,9]. The drawback of this data transmission method is low immunity against such factors as low illumination and presence of the alien bodies between the transmitter and the reader.

3.3 The system structure

Fig. 2 shows the structure of the suggested identification system. To get universality and to widen the system potential users, it was decided to utilize three technology of the data transfer.

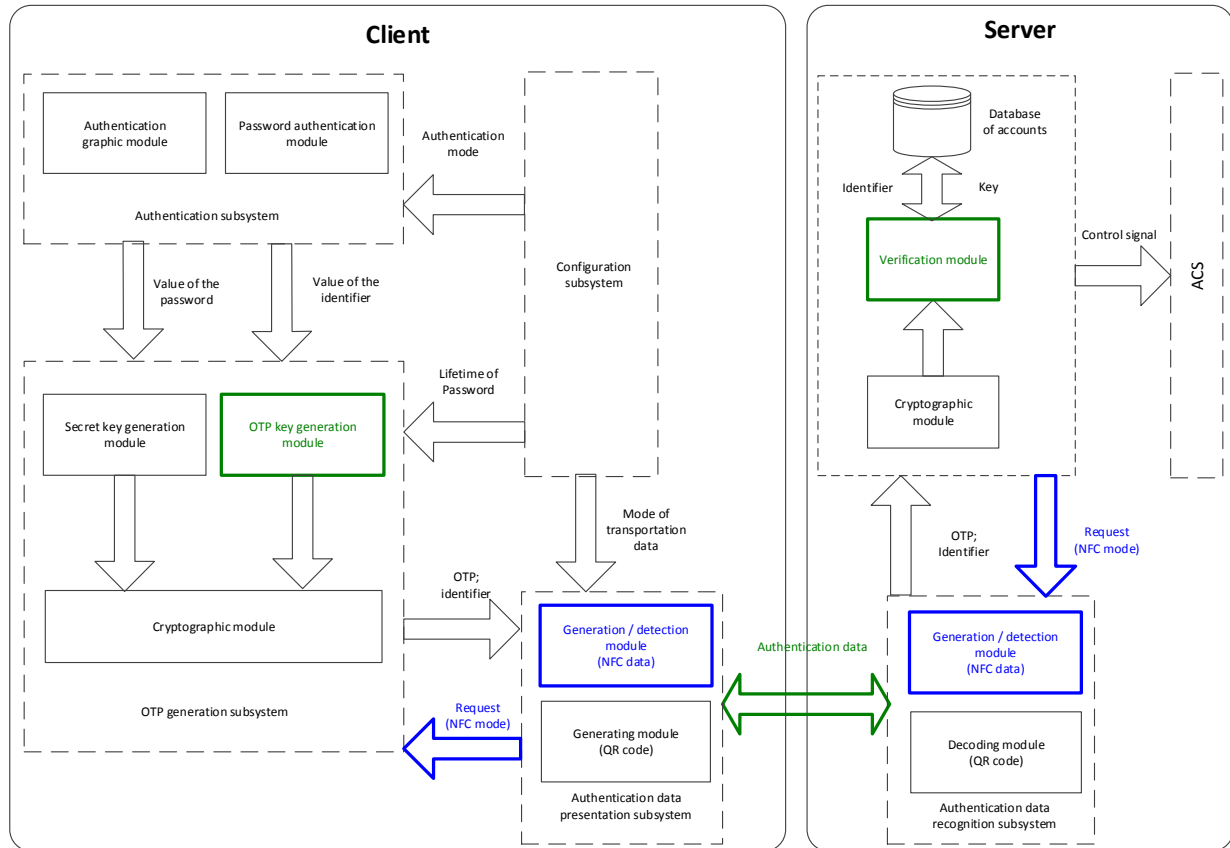


Figure 2. The structure of the designed system

To protect the transmitted data from compromentation, the autentication mechanism based on the one-time authorization code technology in the " synchronization in time" mode is suggested. Function $F(1)$ describes the process of the authentication code receiving [10]:

$$F(u, p, t) = Q[u * ER[H(p), l](u \oplus t)], \quad (1)$$

where u – the user identifier;

p – a group from the secret key components;

t – the current temporal mark;

$Q(x)$ – the message x coding operation to pass to the reading device;

$*, \oplus$ – the operation of concatenation with some dividers;

$E_k(x)$ – the operation of encoding message x at key k ;

$R(x, y)$ – the operation of the secret key formation using input line x according to demands y to the secret key in the process of the utilized mode of encoding;

$H(x)$ – the operation of the x line hashing;

l – demands to the secret key in the process of the utilized mode of encoding.

The second factor of the authentication is protection from the unauthorized access to the application using the modern method of graphic pass keys. The graphic pass key has two components complementing each other. It includes an image from the user multi-media library and a group of signs (gestures), put above the image. Using the private images makes security more reliable and helps to remember the pass-key.

4. Conclusion

The main advantage of the discussed system is the author's idea of realizing the procedure of identification without providing the subject of access with additional physical objects still keeping the opportunity of the authentication parameters variation to meet the demands of the object security policy. The author suggests using mobile platforms and utilizing their technologies. Certainly, the author does not suggest the full replacement of the traditional electronic passes by the mobile access at the moment. Still such systems could be the convenient addition to the ACS, providing new opportunities and advantages.

5. Acknowledgments

This work was supported by the Ministry of Education and Science of the Russian Federation within the 1.3 federal program research and development in priority areas of the scientific-technological complex of Russia for 2014-2020 (grant agreement 14.577.21.0172 of October 27, 2015; identifier RFMEFI57715X0172).

References

- [1] Bezzateev S V, Zharinov R F, Petrov V I and Zybin V A 2015 *Information Security Problems. Computer Systems* **4** 17–22
- [2] Desnitsky V A and Kotenko I V 2016 *XIX IEEE Int. Conf. on Soft Computing and Measurements (St. Petersburg)* pp 481-83
- [3] Munch-Ellingsen A, Karlsen A, Andersen A and Akselsen S 2015 *First Conf. Mobile and Secure Services (Gainesville)* pp 1-6
- [4] Kuliesius F and Dangovas V 2016 *Eighth Int. Conf. on Ubiquitous and Future Networks (Vienna)* pp 894-99
- [5] Birichevskij A R 2016 *SPIIRAS Proc.* **46** 128–38
- [6] Fan W, Huang W, Zhang Z, Wang Y and Sun D 2015 *Trustcom/BigDataSE/ISPA* pp 1324-28
- [7] Fortat F, Laurent M and Simatic M 2015 *Int. Workshop Network and Systems Support for Games (Zagreb)* pp 1-3
- [8] Yin L R, Zhou J and Hsu M K 2015 *Computer Software and Applications Conf. (Taichung)* pp 678–79
- [9] Markman A, Javidi B and Tehranipoor M 2014 *IEEE Photonics Journal* **6** 1–9
- [10] Iskhakov A Y 2014 *Bezopasnost Informatsionnykh Tekhnology* **3** 97–102