Handheld Wireless Authentication Key and Secure Documents Storage for the Internet of Everything

Maria Komar
Tampere University of Technology
Tampere, Finland
Yaroslavl State University
Yaroslavl, Russia
mariia.komar@tut.fi

Sviatoslav Edelev
University of Goettingen
Goettingen, Germany,
sedelev@informatik.uni-goettingen.de

Yevgeni Koucheryavy
Tampere University of Technology
Tampere, Finland
yk@cs.tut.fi

***Abstract*—In this paper, a novel approach for user authentication in Internet of Everything, called "wireless key" is studied. While the majority of existing solutions suggest a wireless key to be a battery-powered device with considerable computational power, we propose to use passive NFC tags instead. In our approach, all the computations are performed by the service the user is authenticating to and thus no computational power and no battery on the key side is required. This approach allows minimizing the device size and significantly reducing the costs. To ensure security of data stored on the tag we propose a transparent data encryption mechanism constructed on top of strong cryptographic primitives. In addition to the authentication-related feature, we have designed a system that enables secure storage of documents on the same tag making it capable of saving ID cards, bank cards, licenses, etc. The presented approach allows on-the-fly validation of any stored document by the entity that issued it as well as by any other entity granted such permissions. Correctness and a security level of the system have been assessed via the analytical study and validated through a hardware prototype. The algorithms and protocols described in the paper are also applicable to any other carrier technology including Bluetooth Low Energy and Wireless USB.**

I. Introduction

The world is now moving far beyond standalone personal computers towards a new paradigm where all the devices are connected. Today the huge growth of smart home devices population, originally being a key trend of the "Internet-of-Everything" concept, is accompanied by appearance of wearable computers [1], connected vehicles and intelligent transportation systems. According to Cisco, this market is going to reach the value of 50 billions devices by 2020 [3]. IoT paradigm affects all areas of human activities from commonly used computer networks [2] to Smart Homes, Intra-device Communications [31], Internet of Nano Things [4], [6], [7] and even such futuristic concepts as Organ-on-a-Chip [10], [13]. Despite the fact that a substantial amount of links between these devices are to be human-unattended, the end user still plays a key role in the deployed infrastructure as the aggregated information from sensors, smart meters, actuators will finally be delivered to the end user. Meanwhile, end user can control the behaviour of these systems by sending commands or requests. Therefore, a convenient, reliable and secure technique for user-to-infrastructure communication is required. Following the same source [3], since the capacity of mobile networks tends to rapidly grow [18], [20], information security becomes a key challenge for future systems design [11]. With respect to large massifs of sensitive data being stored and processed online [5], a trusted and user-friendly method of data access control has to be implemented [19].

One of the key problem when one proposes an authentication technique applicable for Internet-of-Everything is as follows. Despite the fact that lots of devices are to be connected with each other, they do not form a fully connected graph. In particular, an ATM in a supermarket is very unlikely to be connected with a smart home system in a house. So, smart devices in the environment are to be distributed into several big independent clusters. Therefore, the authentication techniques for such infrastructure have to be designed accordingly.

Unfortunately, the overwhelming majority of ways User can be authenticated is not fully scalable. In particular, the "know"-based approaches, such as text passwords or emerging graphical passwords [8], force the user (due to human memory limitations) either to apply the same password for all the systems, to generate passwords in a similar and easy-to-remember way, or even to create notes. In this case, attacker can steal the notes or crack a couple of weak electronic systems and then easily guess the rest of user's passwords observing the pattern.

The biometric approach does neither seem to be a reliable solution. For example, the fingerprinting login technique for Apple iPhone was cracked within 24 hours after the release date [12]. Moreover, a huge privacy-related problem is concerned: how to motivate users to provide their identity information to third parties? Even when manufactures claim not to synchronize this data with online services and store it in an encrypted manner inside the Trusted Platform Module (TPM [9]), such kinds of deals require much higher level of trust, than a person usually has to a payment terminal in the Internet Cafe.

A widely used approach to authenticate the end user through the third party raises the same question of trust: how to be assured that the intermediate service will not disclose private data to other parties. Moreover, storage of authentication data on a single service makes it subject to the increased amount of interest from the attackers' side. Within some time, such kind of service also becomes a so-called *Single Point of Failure* — once such a service is shutdown, users are unable to authenticate to other services anymore [15].

Open questions in the applicability of existing authentication techniques resulted in the proposal of several novel paradigms for user authentication to multiple independent information systems. One of the most promising approaches is related to the idea of wireless keys.

Being motivated by a set of issues in all the conventional authentication techniques, the group of companies and foundations called FIDO Alliance [27] with Google, Lenovo and PayPal on board, is working towards design, implementation and deployment of a simple, easy-to-use and strong authentication scheme. One of their main research tracks is a wireless key development. The idea of a wireless key approach is to introduce a device that can store all the user's passphrases inside and send one of them wirelessly to the corresponding service during the authentication procedure. In order not to compromise the security level, the device has to perform a two-side mutual authentication with the service instead of a one-side authentication in conventional systems. Otherwise, attacker can perform a masquerade attack [14] pretending to be the named service, initiate the authentication phase and get the passphrase s/he is interested in. Therefore, the current wireless key design suggests it to be a small computer with its own memory, computational and power resources, wireless connectivity and charging interface.

However, battery-powered devices performing mutual authentication has natural drawbacks: increased device costs and limited battery lifetime. The latter may result in an inability to enter the own house because of the discharged key. Therefore, the existing design of wireless keys is very unlikely to become a part of the usual everyday life. Hence, the aim to design a small, cheap, secure and easy-to-use solution is still not reached.

Moreover, existing approaches do not provide solutions on how to verify user credentials by an entity different from the one that issued the document. For example, when the digital ID issued by the University has to be verified by a ticket inspector in an intercity train to provide a discount. Or, when a digital driver license has to be checked for the identity proof for bank card payment.

In this paper, we present a novel approach to design a wireless key for user authentication to multiple independent systems. To make it user-friendly, we propose user credentials as well as digital documents to be stored on an NFC tag as cheap and battery-free devices. Though sensitive information is stored on a single user device, confidentiality of data is guaranteed by the specific encryption scheme based on combination of strong cryptographic primitives from both symmetric and asymmetric cryptography. Moreover, the proposed data integrity technique enables validation of the user identity by a third party, hence, making our scheme applicable for secure document storage. In order to be able to use NFC tags as user key devices, cryptographical schemes are designed so that no computation on the tag side is required. As a result, the proposed solution is cost-efficient, convenient, scalable, and secure. It was assessed for the security level and prototyped.

The rest of the paper is organised as follows. Section II presents the State-of-the-Art survey of security and privacy systems for IoE-aware infrastructure being proposed so far. Examples of possible applications and user scenarios for the proposed system as well as formal requirements for the access control scheme are given in Section III. Section IV is focused on system architecture, proposed access control scheme and utilised cryptographic primitives, while Section V illustrates the technical aspects of the scheme reference implementation in our test bench including both hardware and software parts. Assessment of security level provided by our solution is performed in Section VI. Finally, the qualitative comparison with alternative approaches is summarised in Section VII. The paper ends with some conclusion remarks.

II. Related work

In this section, we describe and analyse established approaches for user authentication to multiple information systems (IS). Within the last few years, with a rapidly growing number of services and devices requiring authentication on a daily basis, the following approaches for user authentication to heterogeneous systems were established:

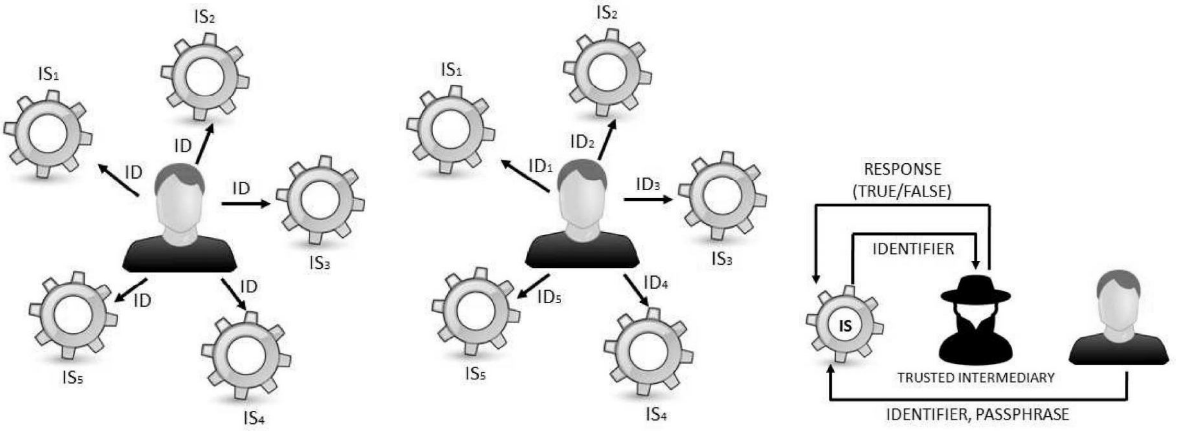
1) Solutions with a single identifier and single key information for all ISs.
2) Solutions with different identifiers, key sequences and authentication methods for different ISs.
3) Solutions with a trusted third party involved.

Of special interest for us are solutions with a portable object as an internal secure repository of identifiers and key sequences for ISs. We thus separately define them as

4a) Non-interactive – the user is not involved into the authentication process.
4b) Interactive – the user is directly involved into the authentication process (s/he selects the IS to access, enters a PIN or password, etc.)

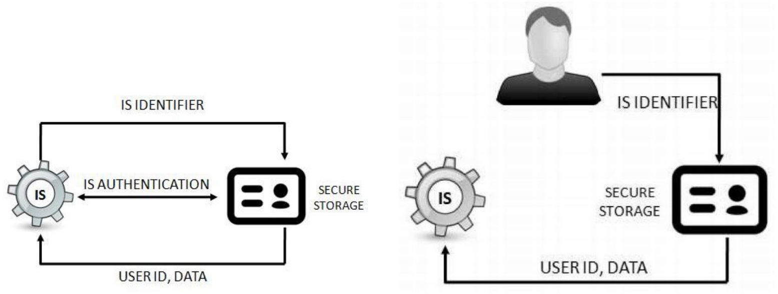
Though it is obvious that using the same key information for authentication to multiple ISs (approach 1) is not secure, this naïve manner is still widely used. The reason for that is convenience for the user because s/he has to memorize only one key sequence or present only one identification document. While in the latter case the user may disclose a part of private data that the requesting side should not know, in both cases protection of the authentication data should be arranged on the system side. In case of secret information disclosure through vulnerability in one of the ISs, the attacker will get access to all the others. The same applies for the biometrics-based authentication when the user may present the same biometrical data (such as a fingerprint, iris scan, voice pattern) to different ISs. Considering the discovered vulnerabilities of such systems [16], this approach does not seem promising from the security point of view.

The main idea of the second approach is to create a unique pair "identifier – key sequence" for every IS meaning that duplication of neither identifiers nor key sequences in different pairs occurs. A typical example of such an approach is to have different access keys to different areas or showing different



(a) Common identifier for different information systems (b) Different identifiers for different information systems (c) Solutions with a trusted third party involved

Fig. 1. Approaches for user authentication (1)



(a) Non-interactive (b) Interactive

Fig. 2. Approaches for user authentication (2)

loyalty cards in different retail stores. This approach is reliable because breaking a single IS does not allow the attacker to get access to the others. However, the implementation imposes additional restrictions to the user. For the knowledge-based techniques such as text passwords or becoming popular graphical passwords ([8], [28], for a survey see: [29]) the main limitation is a human memory. For the user it is difficult to memorize several secure passwords, unrelated with each other and with user-associated information. It leads to the situation that similar or easy-to-remember passwords are used, or kept on a note, thus becoming available for the people around. Being aware of humans nature, an adversary once getting access to one of the user's passwords (for example, through a vulnerability in one of the authentication services) can guess the others. If secret information is stored on a portable object, the user has to hold a number of physical keys or smart-cards, which is not convenient for him.

The third of the above-mentioned approaches involves a trusted third party that validates the key sequences instead of the IS subsystem, and reports to the IS only the validation result: "true/false". Typical examples of the systems that implement this approach are OAuth [30] service providers such as Google Wallet, Amazon Check-Out, PayPal services, Facebook, or password managers. However, involvement of a trusted third party imposes the same type of vulnerability as the first approach does – the existence of a single point of failure. Moreover, this approach raises a question of trust to the third-party service and its obligations not to disclose user private data to other parties.

In the last approach, in order to replace the third party authority, a unified portable bearer of identifiers and key sequences is used. However, the main challenge is to separate access to key sequences between different ISs. Existing solutions of this class widely use the following two ways to address this challenge: either to implement the two-way mutual authentication (4a) or to perform authentication in an interactive mode (4b).

In the first case (4a), Kerberos [32] or its modifications are commonly used, where the low power CPU is placed to the side of the device with key sequences. For example, the current design by FIDO Alliance [27] suggests the key to be a small computer with its own CPU, memory, battery, wireless data interface and wired/wireless charging interface. The presence of all these components is required in order to perform a lightweight mutual authentication protocol, such as OAuth [30], LMAP [33] or OPACITY [34]. However, such solutions are not applicable to the wide range of tasks because of the low computational power of the device core and the need to use a simplified version of a protocol with a reduced key length, resulting in a lower security level. Additionally, no long-term battery exists enough to support continuously such heavy computational tasks.

In the second case (4b), a number of secure media solutions use the interactive mode to solve the problem of separating data access between ISs. In particular, the universal electronic card [36] makes the user enter different pin-codes on the terminal to access different services such as banking, governmental services, or electronic signature. Similarly, in OnlyCoin project [38] before the transaction takes place the user has to manually select the credit or membership card that s/he wants to use for payment. Despite the security advantages in the key sequences separation scheme, the user is forced to do extra work during authentication. Thus, the resulting solution being adequately secure is not user friendly.

III. Applications and system requirements

A. *Possible user scenarios*

Systems of 4a-type have many different applications. From ordinary user's point of view it is convenient to have a single ticket for all events starting from rock concert ending with ticket for train. It allows not to carry out a huge amount of different papers (or files stored on some flash drive and/or hard disk). There are several mobile applications that allow to store e-versions of tickets in mobile phone's memory. It can be a good solution, but when mobile phone is discharged the problem occurs. On the other hand 4a-type solutions without battery power are attractive. Moreover, such solutions can be applied for storing some bills and other financial documents.

The evolution of previous idea is to store authorized copies of all user's documents (passport, driving license, university diploma etc.). It is suitable for situations when user would like to confirm his/her right to enter a building or get a student discount in the cafeteria using the only device (such as card, bracelet, trinket, etc.) in all situations. On the one hand, user not forced to always carry a large amount of paper-based documents that s/he may lose or damage at any time, on the other hand s/he is able to obtain necessary data from documents or confirm his/her rights any time. This considerations leads to idea of secure documents storage creation. It is important to note, that documents stored on user's device can be read and modified only by organization that eligible to do it. For example, information in authorized copy of student card can be changed by university issued the card only.

One more idea based on considerations mentioned above is to store all passphrases assumed with different systems in one place securely and transmit them on wires/wirelessly. It allows user not to enter passphrases every time and not to remember large amount of different words/pictures/digits sequences. Moreover, such approach could increase security level due to ability to store longer chains of characters. Hereby the idea of wireless key is introduced. This concept becomes popular and many companies are interested in appearance of cheap battery-free solution that can provide proper security level.

Last two ideas are well suited for Internet of Things concept. Systems like Smart Cities, Smart Homes, Smart Spaces, Machine-to-Machine Communication systems [35], [37], [39], [40], [43] became more and more popular. There are a lot of sensors and transducers, and in some amount of them user authentication required. However in situation when number of sensors around us more than number of people at the Earth entering passwords for all this systems is not acceptable. Besides, systems more intelligent than for example temperature probe require extra data. Solutions that can store passphrases and documents fit well for such tasks. To summarize, we can formulate a set of requirements for secure documents and passphrases storages that would be applicable for Internet of Things solutions.

B. *Requirements for the security system*

In order to develop a secure, scalable and user-friendly system which satisfies the needs for user authentication to the IoT infrastructure, the following set of requirements should be met:

1) User authentication information (hereinafter: a Document) should be stored on a portable easy-to-carry (easy-to-wear) device (hereinafter: a Tag) with no power supply.
2) A User should be able to read Documents from his/her Tag.
3) An Infrastructural unit (hereinafter: a Department) should be able to issue user-specific Documents.
4) A Department should be able to read and modify issued by this department Documents from User Tags.
5) A Department can delegate other Department(s) right to read issued by this Department Documents from User Tags.
6) Stored on the tag Documents should be integrity-protected, i.e. only the issuing Department should be able to modify them.
7) During the authentication phase no additional actions performed by the User are required (the User is not required to enter a password or to explicitly allow access to the Tag).
8) Users are not able to read Documents stored on other Users's Tags even if they have physical access to memory of tags.
9) If the reading access was not delegated, the Department can not get access to the stored on the User tag Documents issued by other Departments, even if it has physical access to the memory of the tag.
10) The User is not able to modify Documents stored on his/her Tag

IV. Many-to-many access control scheme

In this section scheme allows many users and departments securely exchange data between concerned nodes is described in terms of Users, Departments, Certification Centers and documents stored on tags.

A. *Network topology and nodes classification*

We suppose that the network consists of nodes of three types. First of all, there are N Users that may have home PCs/mobile devices with computational power. This is not a mandatory but a desirable condition, allowing to take an advantage of the scheme with the maximum benefits for Users. Each User has his/her own device, that is able to store some amount of data associated with the systems the User has to communicate with. Secondly, there are M Departments representing information systems (such as payment terminals in shops, banks, public transport, etc.) (see Fig. 3(a)). For their operation, Departments require terminals with computational power, some amount of memory and (in particular cases) Internet connection. The third type of nodes are Certification Centres (CC). They generate public and secret keys for new Users and Departments. In some cases Certification Centres (CC) and Departments may be the same organisations.

B. Core idea and file structure on a tag.

Each User and Department has own secret and public keys. Every User has a tag that stores his/her identifiers and passphrases for different systems and/or authorized copies of documents. It is important to note, that the data is stored in an encrypted way wherein pieces of data affiliated with different Departments are encrypted with different keys generated on the basis of User's and Department's keys. Moreover, every document is signed by the Department that issued it. It means that attacker (or a User) cannot modify any document without consent of the Department that issued it, since unauthorized changes make the digital signature invalid. For the efficiency purposes we propose to use an XML-based file structure on the storage device (see Fig. 3(b)), where documents are accomplished by a digital signature and encrypted using a strong symmetric encryption algorithm (e.g. AES-256 [17]) with different encryption keys (see Fig. 3(c)).Moreover, Departments are able to give other Departments the permission to read issued by them documents but not to change them. Comparing to online documents storages, the presented approach provides higher level of usability because the device could be used even in the cases when the Internet connection is not available. In addition, such a system achieves the ultimate level of privacy due to the fact that all the sensitive data are stored locally in encrypted manner and not synchronized with any online system outside the User's network.

C. Procedure description

The complete description of the access control scheme could be divided into seven phases. Certification Centers (CC) take part in stages 1-3 only when new Users and Departments are added to the system. The other operations (stages 4-7) are performed without interaction with CC. So, in contradiction to majority of existing systems, no third-parties are required during communication between User and Department.

1) Setup. During the setup procedure, all Certification Centers generate and publish their system Public Keys c_i. After that, every CC generates a Master Secret Key a_i, to be stored privately by CC and used only to generate secret keys for Users and Departments. Both c_i and a_i must be large prime numbers.

2) Include a new Department. When a Department i appears in the system, it requests a unique identifiers DID_{i,CC_k} from all the Certification Centers it has to operate with (subset of all the CCs). Responding to this request, every CC selects a previously unused large prime $z < c_k$ and sets DID_{i,CC_k} being equal to z. In addition, CC generates an encryption key $DKey_{i,CC_k}$ for the new node using the equation 1.

$$DKey_{i,CC_k} = (a_k)^{DID_{i,CC_k}} \mod c_k \quad (1)$$

After key generation, CC delivers pair $DID_{i,CC_k}; DKey_{i,CC_k}$ to the new Department. At this stage the secure and reliable link is required between CC and Department for initial key establishment. Once the procedure is finished, the Department saves locally its DID_{i,CC_k} and $DKey_{i,CC_k}$. Both of these values will be further used during the data access procedure.

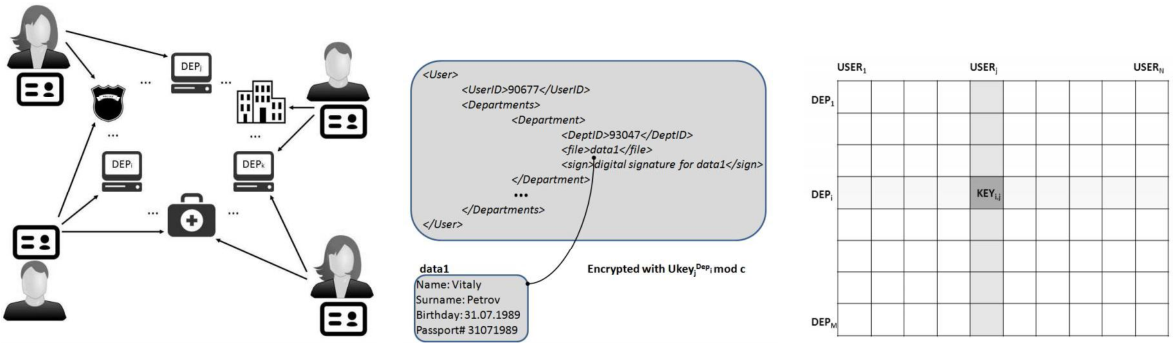
After the connection is terminated, Department locally generates a pair of signature keys: $SEC_i; PUB_i$ based on public key cryptography algorithm. Finally, a set of identifications DID_{i,CC_1}; ... DID_{i,CC_n};, encryption keys $DKey_{i,CC_1}$; ... $DKey_{i,CC_n}$; and $SEC_i; PUB_i$ is stored on the Department side. SEC_i would be further used to generate a digital signature for documents, issued by this Department, while all the rest values are needed to decrypt the document and verify the signature (see Item 7 for details).

3) Include new User. During this procedure the initial configuration of wearable document storage has to be performed. To enable the configuration, the device has to be connected for short time to a trusted terminal (e.g. User home computer or smartphone), that has a protected link to CC (for example, SSL connection authenticated by CC certificate on one side and User's OpenID [21]). Once the connection is established, User has to select his/her own password pwd for the device and remember it or store in a secure location. Then, similar to the previous procedure, User receives its UID_{j,CC_k} equal to a previously unused large prime $z' < c_k$ from every CC, User is going to operate with. The User secret keys $UKey_{j,CC_k}$ are generated by CCs via equation 2 and also sent to the User.

$$UKey_{j,CC_k} = (a_k)^{UID_{j,CC_k}} \mod c_k \quad (2)$$

The list of UID_{j,CC_k} sorted by n is to be stored on the document storage in a plaintext mode, while a set of corresponding secret keys is to be encrypted with an AES-256 [17] symmetric cypher on a key derived from pwd by SHA-256 [22] hash function.

4) Grant read access. When all the pre-configuration is already performed it might be beneficial to share the reading access privileges between departments (e.g. a University would like to share the ability to verify student cards to the public transportation operator). This feature is also supported by the proposed access control scheme. If one Department (Source) would like to grand read access to another Department (Recipient), Source has just to share a triple $DID_{i,CC_k}; DKey_{i,CC_k}; PUB_i$, related to selected documents, with the Recipient. One the operation is over, Recipient is capable of reading and validating the documents, issued by the Source (either all or given subset, depending on how many triples veer shared between departments). At the same time, Source is still the only entity capable of issuing its

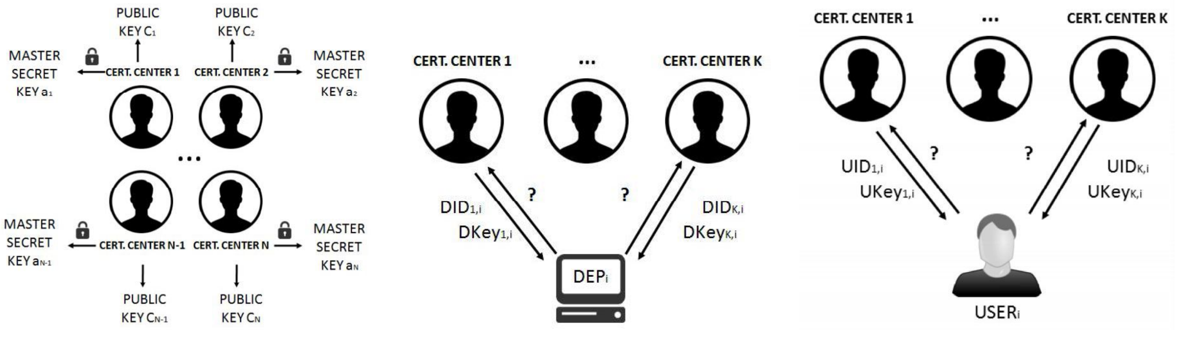


```
<User>
        <UserID>90677</UserID>
        <Departments>
                <Department>
                        <DeptID>93047</DeptID>
                        <file>data1</file>
                        <sign>digital signature for data1</sign>
                </Department>
                ...
        </Departments>
</User>
```

Name: Vitaly
Surname: Petrov
Birthday: 31.07.1989
Passport# 31071989

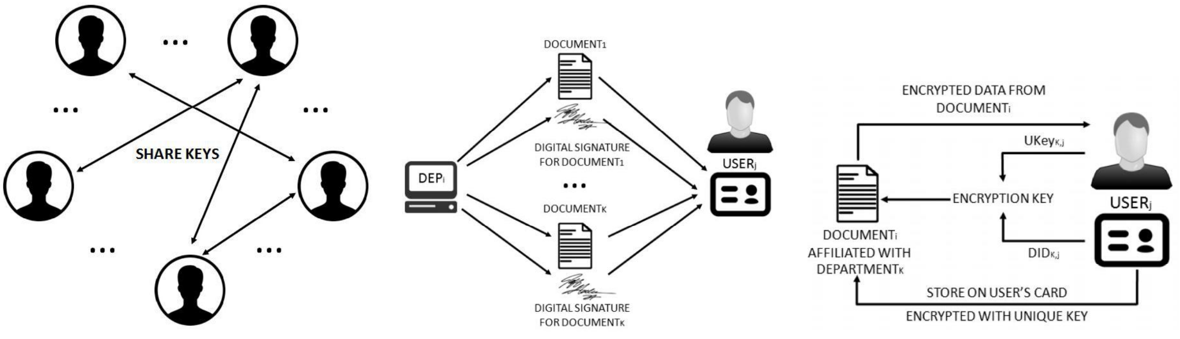
(a) System topology (b) File structure on a tag (c) Matrix of encryption keys

Fig. 3. Common system topology, file structure on a tag and matrix of encryption keys



(a) Setup phase (b) Include new Department phase (c) Include new User phase

Fig. 4. Different phases of access control schemes (1)


...
SHARE KEYS
DOCUMENT$_1$
DIGITAL SIGNATURE FOR DOCUMENT$_1$
...
DOCUMENT$_K$
DIGITAL SIGNATURE FOR DOCUMENT$_K$
DEP$_i$
USER$_j$
ENCRYPTED DATA FROM DOCUMENT$_i$
UKey$_{K,j}$
ENCRYPTION KEY
USER$_j$
DOCUMENT$_i$ AFFILIATED WITH DEPARTMENT$_K$
DID$_{K,j}$
STORE ON USER'S CARD
ENCRYPTED WITH UNIQUE KEY

(a) Grant read access phase (b) Add new document phase (c) Read the document on User terminal phase

Fig. 5. Different phases of access control schemes (2)

own documents, due to the fact, SEC_i is not shared. As such, Recipient can verify signatures but cannot create them.

5) <u>Add new document.</u> Department can issue as many documents as required for a selected User by the following procedure. First of all, issued document d has to be signed with the department secret signature key: $s = sign(SEC_i, d)$. Then, Department reads the User ID UID_{j,CC_i} from the device and calculates a round encryption key $KEY_{k,i,j}$ by equation 3. Finally, the pair $d; s$ is to be encrypted using strong symmetric encryption (e.g. AES-256) on a round key $KEY_{k,i,j}$ and stored on the device.

$$KEY_{k,i,j} = DKey_{i,CC_k}^{UID_{j,CC_k}} \mod c_k. \quad (3)$$

6) *<u>Read the document on User terminal.</u>* One of the key features of the proposed system is that User can easily get access to all his/her documents calculates a round encryption key $KEY_{k,i,j}$ by equation 4. Only thing that user needs to know to generate this key is a single password pwd (see Item 3). At the same time, the value of this password does not become a *single point of failure* due to the fact, that User is not able to modify the documents without direct permission of the Department who has issued it. In particularly, the correct value of signature secret key SEC_i is

required. Let us recall, this key is generated locally on the Department without any interaction with either Users of CCs. This key is also never disclosed to other Departments even during the *Grant read access* procedure, described in Item 4

$$KEY_{k,i,j} = UKey_{i,CC_k}^{DID_{j,CC_k}} \mod c_k. \qquad (4)$$

7) *Read and validate the document on Department terminal.* This procedure is assumed being one of the most frequent during the system lifetime. When User has to prove his/her identity to a third party — Department — s/he transmits the triple $UID_{j,CC_k}; E(d); E(s)$, where $E(d)$ denotes for the document encrypted with round key $KEY_{k,i,j}$ (see equation 3) and $E(s)$ is the document signature, encrypted with the same key.

   Once this triple is successfully received by the Department, it can derive the round encryption key $KEY_{k,i,j}$ using equation 3. Then, the pair $E(d); E(s)$ is to be decrypted. Finally, Department can verify the digital signature s by comparing it to $s' = sign(SEC_i, d)$.

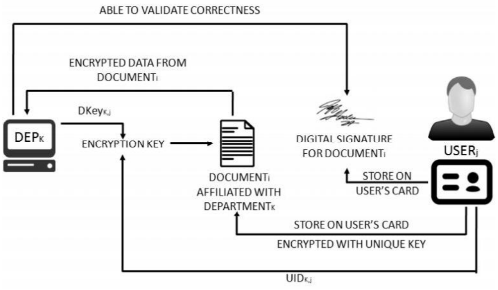

ABLE TO VALIDATE CORRECTNESS
ENCRYPTED DATA FROM DOCUMENTi
DKeyK,j
DEPK
ENCRYPTION KEY
DOCUMENTi AFFILIATED WITH DEPARTMENTK
DIGITAL SIGNATURE FOR DOCUMENTi
USERj
STORE ON USER'S CARD
STORE ON USER'S CARD
ENCRYPTED WITH UNIQUE KEY
UIDK,j

Fig. 6. Read and validate the document on Department terminal phase

Thereby the proposed system allows both Users and Departments access all required documents securely (see section VI for more information) and conveniently. Besides User doesn't need any computation and battery power on tag (and require a home PC/smartphone only in cases when s/he would like to read his/her own documents) and there is no need to remember huge amount of passwords. Departments are not have to store huge amount of data and secret keys on their side, that increases security level.

V. Prototype description

In order to demonstrate feasibility of the proposed scheme we have developed two prototypes: based on NFC-tags and on USB-tokens as the storage types. Both wired and wireless solutions are fully reliable as even wireless links are suitable for security-sensitive applications [23]. The NFC-based prototype consists of an NFC-reader Identive SCL3711, NFC-tags DESFire EV1 4K and a software implementing the proposed scheme. Software was developed for Windows OS and is written on C#. Interaction with the NFC-reader takes place using a native wrapper library SCM_NFC.dll. The library provides access to the high-level functions such as tag scanning, reading and writing (available only in the text mode).

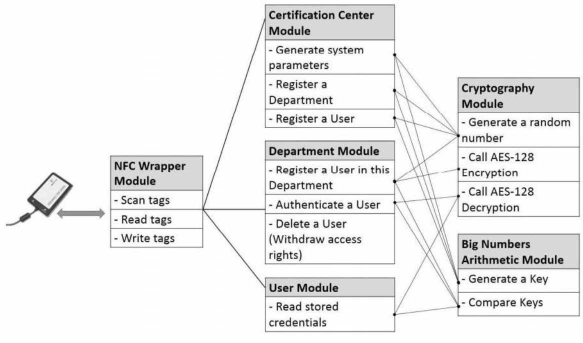
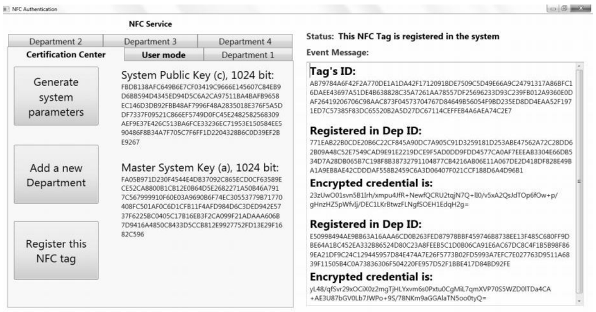

Certification Center Module
- Generate system parameters
- Register a Department
- Register a User
NFC Wrapper Module
- Scan tags
- Read tags
- Write tags
Department Module
- Register a User in this Department
- Authenticate a User
- Delete a User (Withdraw access rights)
User Module
- Read stored credentials
Cryptography Module
- Generate a random number
- Call AES-128 Encryption
- Call AES-128 Decryption
Big Numbers Arithmetic Module
- Generate a Key
- Compare Keys

Fig. 7. Software architecture

The developed prototype has three modes of operation representing elements of the system topology: Certification Center, Department and User modes. In the Certification Center (CC) module, system parameters such as a Master Secret Key *a* and a Public System Key *c* (see 1) are generated. These parameters are stored on the CC side. In order to provide high security level keys should be 4096 bit, however in the NFC-based prototype the size was reduced to 1024 bit to allow more records on the tag. In the next step, the Departments are added to the system: CC generates their IDs (Section IV-C, step 2) and secret keys (formula 1), and transmits this information together with the System Key to the Department. The last step is to add Users to the system: CC generates a User ID (Section IV-C, step 3) and the secret key (formula 2), and transmits them together with the System Key to the User. The User ID is written the Tag, other parameters are stored separately, for example, on the User's laptop. The result of these steps is show on Fig. 8:

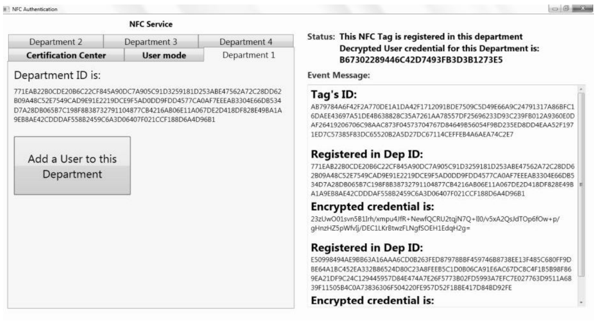


```
System Public Key (c), 1024 bit:
FBDB138AFC649B6E7CF03419C9666E145607C84EB9
D6BB594D4345ED94D5C6A2CA97511BA4BAFB9658
EC146D3DB92FBB48AF7996F48A2835018E376F5A5D
DF7337F09521C866EF5749D0FC45E2482582568309
AEF9E37E426C513BA6FCE33236EC71953E150584EE5
90486F8B34A7F705C7F6FF1D2204328B6C0D39EF2B
E9267

Master System Key (a), 1024 bit:
FA05B971D230F4544E4DB37092C865ECD0CF63589E
CE52CA8800B1CB12E0B64D5E2682271A50B46A791
7C567999910F60E03A9690B6F74EC30553779B71770
408FC501AF0C6D1CFB11F4AFD984D6C3DED942E57
37F6225BC0405C17B16EB3F2CA099F21ADAAA606B
7D9416A4850C8433D5CCB812E9927752FD13E29F16
82C596

Status:  This NFC Tag is registered in the system
Event Message:
Tag's ID:
AB79784A6F42F2A770DE1A1DA42F1712091BDE7509C5D49E66A9C24791317A86BFC1
6DAEE43697A51DE4B638828C35A7261AA78557DF25696233D93C239FB012A9360E0D
AF26419206706C98AAC873F04573704767D84649B56054F9BD235ED8DD4EAA52F197
1ED7C57385F83DC65520B2A5D27DC67114CEFFEB4A6AEA74C2E7

Registered in Dep ID:
771EAB22B0CDE20B6C22CF845A90DC7A905C91D3259181D253ABE47562A72C28DD6
2B09A48C52E7549CAD9E91E2219DCE9F5AD0DD9FDD4577CA0AF7EEEAB3304E66DB5
34D7A28DB065B7C198F8B38732791104877CB4216AB06E11A067DE2D418DF828E49B
A1A9EB8AE42CDDDAF558B2459C6A3D06407F021CCF188D6A4D96B1
Encrypted credential is:
23zUwO01svn5B1Irh/xmpu4JfR+NewfQCRU2tqjN7Q+lI0/v5xA2QsJdTOp6fOw+p/
gHnzHZ5pWfvIj/DEC1LKrBtwzFLNgfSOEH1EdqH2g=

Registered in Dep ID:
E50998494AE9BB63A16AAA6CD0B263FED87978BBF459746B8738EE13F485C680FF9D
BE64A1BC452EA332B86524D80C23A8FEEB5C1D0B06CA91E6AC67DC8C4F1B5B98F86
9EA21DF9C24C129445957D84E474A7E26F5773B02FD5993A7EFC7E027763D9511A68
39F11505B4C0A73836306F504220FE957D52F1BBE417D84BD92FE
Encrypted credential is:
yL48/qfSvr29xOCiX0z2mgTjHLYxvm6s0Pxtu0CgMiL7qmXVP70S5WZD0ITDa4CA
+AE3U87bGV0Lb7JWPo+9S/78NKm9aGGAlaTN5oo0tyQ=
```

Fig. 8. Certification Center mode

In the Department mode, Users are registered to the Department meaning that the Department authorizes certain Tags. Authorization is performed by generating a User credential (16 byte). Hash of this credential together with the User ID is stored on the Department side. The User credential encrypted with AES-128 encryption (where the encryption key is calculated from formula 3) together with the Department ID is sent to the User. Once the User starts authenticating himself in the Department, the User attaches his/her Tag to the Department's Reader. The Department reads a User ID and an encrypted credential corresponding to this Department from the Tag. The User credential is decrypted using the key from formula 3, hashed and compared with the hash stored in the

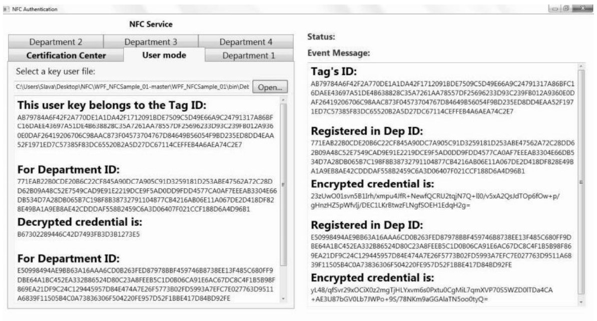
Department Database (see Fig. 9). To withdraw authorization rights from particular User, the Department deletes a record with User credentials from its database.



```
Department ID is:
771EAB22B0CDE20B6C22CF845A90DC7A905C91D3259181D253ABE47562A72C28DD62
B09A48C52E7549CAD9E91E2219DCE9F5AD0DD9FDD4577CA0AF7EEEAB3304E66DB534
D7A28DB065B7C198F8B38732791104877CB4216AB06E11A067DE2D418DF828E49BA1A
9EB8AE42CDDDAF558B2459C6A3D06407F021CCF188D6A4D96B1

Status: This NFC Tag is registered in this department
        Decrypted User credential for this Department is:
        B67302289446C42D7493FB3D3B1273E5
Event Message:
Tag's ID:
AB79784A6F42F2A770DE1A1DA42F1712091BDE7509C5D49E66A9C24791317A86BFC1
6DAEE43697A51DE4B638828C35A7261AA78557DF25696233D93C239FB012A9360E0D
AF26419206706C98AAC873F04573704767D84649B56054F9BD235ED8DD4EAA52F197
1ED7C57385F83DC65520B2A5D27DC67114CEFFEB4A6AEA74C2E7

Registered in Dep ID:
771EAB22B0CDE20B6C22CF845A90DC7A905C91D3259181D253ABE47562A72C28DD6
2B09A48C52E7549CAD9E91E2219DCE9F5AD0DD9FDD4577CA0AF7EEEAB3304E66DB5
34D7A28DB065B7C198F8B38732791104877CB4216AB06E11A067DE2D418DF828E49B
A1A9EB8AE42CDDDAF558B2459C6A3D06407F021CCF188D6A4D96B1
Encrypted credential is:
23zUwO01svn5B1Irh/xmpu4JfR+NewfQCRU2tqjN7Q+lI0/v5xA2QsJdTOp6fOw+p/
gHnzHZ5pWfvIj/DEC1LKrBtwzFLNgfSOEH1EdqH2g=

Registered in Dep ID:
E50998494AE9BB63A16AAA6CD0B263FED87978BBF459746B8738EE13F485C680FF9D
BE64A1BC452EA332B86524D80C23A8FEEB5C1D0B06CA91E6AC67DC8C4F1B5B98F86
9EA21DF9C24C129445957D84E474A7E26F5773B02FD5993A7EFC7E027763D9511A68
39F11505B4C0A73836306F504220FE957D52F1BBE417D84BD92FE
Encrypted credential is:
```

Fig. 9. Department mode

In the User mode, the User is able to read his tag and to decrypt the credentials. The decryption of particular credentials is performed separately for every credential using the User secret key and the Department ID (formula 4). User mode is shown on Fig. 10:



```
Select a key user file:
C:\Users\Slava\Desktop\NFC\WPF_NFCSample_01-master\WPF_NFCSample_01\bin\Det

This user key belongs to the Tag ID:
AB79784A6F42F2A770DE1A1DA42F1712091BDE7509C5D49E66A9C24791317A86BF
C16DAEE43697A51DE4B638828C35A7261AA78557DF25696233D93C239FB012A936
0E0DAF26419206706C98AAC873F04573704767D84649B56054F9BD235ED8DD4EAA
52F1971ED7C57385F83DC65520B2A5D27DC67114CEFFEB4A6AEA74C2E7

For Department ID:
771EAB22B0CDE20B6C22CF845A90DC7A905C91D3259181D253ABE47562A72C28D
D62B09A48C52E7549CAD9E91E2219DCE9F5AD0DD9FDD4577CA0AF7EEEAB3304E66
DB534D7A28DB065B7C198F8B38732791104877CB4216AB06E11A067DE2D418DF82
8E49BA1A9EB8AE42CDDDAF558B2459C6A3D06407F021CCF188D6A4D96B1
Decrypted credential is:
B67302289446C42D7493FB3D3B1273E5

For Department ID:
E50998494AE9BB63A16AAA6CD0B263FED87978BBF459746B8738EE13F485C680FF9
DBE64A1BC452EA332B86524D80C23A8FEEB5C1D0B06CA91E6AC67DC8C4F1B5B98F
869EA21DF9C24C129445957D84E474A7E26F5773B02FD5993A7EFC7E027763D9511
A6839F11505B4C0A73836306F504220FE957D52F1BBE417D84BD92FE

Status:
Event Message:
Tag's ID:
AB79784A6F42F2A770DE1A1DA42F1712091BDE7509C5D49E66A9C24791317A86BFC1
6DAEE43697A51DE4B638828C35A7261AA78557DF25696233D93C239FB012A9360E0D
AF26419206706C98AAC873F04573704767D84649B56054F9BD235ED8DD4EAA52F197
1ED7C57385F83DC65520B2A5D27DC67114CEFFEB4A6AEA74C2E7

Registered in Dep ID:
771EAB22B0CDE20B6C22CF845A90DC7A905C91D3259181D253ABE47562A72C28DD6
2B09A48C52E7549CAD9E91E2219DCE9F5AD0DD9FDD4577CA0AF7EEEAB3304E66DB5
34D7A28DB065B7C198F8B38732791104877CB4216AB06E11A067DE2D418DF828E49B
A1A9EB8AE42CDDDAF558B2459C6A3D06407F021CCF188D6A4D96B1
Encrypted credential is:
23zUwO01svn5B1Irh/xmpu4JfR+NewfQCRU2tqjN7Q+lI0/v5xA2QsJdTOp6fOw+p/
gHnzHZ5pWfvIj/DEC1LKrBtwzFLNgfSOEH1EdqH2g=

Registered in Dep ID:
E50998494AE9BB63A16AAA6CD0B263FED87978BBF459746B8738EE13F485C680FF9D
BE64A1BC452EA332B86524D80C23A8FEEB5C1D0B06CA91E6AC67DC8C4F1B5B98F86
9EA21DF9C24C129445957D84E474A7E26F5773B02FD5993A7EFC7E027763D9511A68
39F11505B4C0A73836306F504220FE957D52F1BBE417D84BD92FE
Encrypted credential is:
yL48/qfSvr29xOCiX0z2mgTjHLYxvm6s0Pxtu0CgMiL7qmXVP70S5WZD0ITDa4CA
+AE3U87bGV0Lb7JWPo+9S/78NKm9aGGAlaTN5oo0tyQ=
```

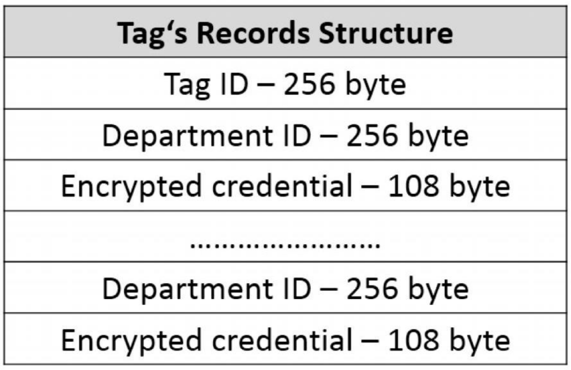
Fig. 10. User mode

The tag records have the following structure (Fig. 11). Therefore, the total memory size taken by the records is

$$256 + (256 + 108) * N \tag{5}$$

bytes, where N is the number of Departments where the Tag is registered. Consequently, for NFC tags used in this prototype (DESFire EV1) with 4K memory, the maximum number of departments to be registered in is 10. This number holds true when information on tags is stored in the bytes representation. However, the native library supplied with the NFC reader does not allow us to read/write in the byte mode. Therefore, we had to store information in the text mode using hexadecimal representation of numbers, thus reducing the maximum number of records.

To provide better storage characteristics, we have developed a prototype based on USB-tokens. The USB-based prototype does not have such strict memory limitations on the user device, therefore, the key size there is kept original (4096 bit), increasing security level. As usb devices are able to store up to 1 TB of data, the maximum amount of user credentials stored on the device increases significantly. The en-/decryption key for AES-256 is taken from the lowest bits of the encryption key from formulas 4 and 3. The rest of functionality is kept the same. The USB-based prototype was developed for Linux OS using Python language and Qt cross-platform library, and was presented in [46].



Tag‘s Records Structure
Tag ID – 256 byte
Department ID – 256 byte
Encrypted credential – 108 byte
....
Department ID – 256 byte
Encrypted credential – 108 byte

Fig. 11. Tag structure

VI. Security and privacy assessment

As was mentioned above, the system must meet security and usability requirements. We can reformulate them as follows:

1) User can read any document stored on his/her card any when and without any restrictions.
2) Department can read documents affiliated with it from any User's card and no additional actions performed by User are required (User need not enter password or allow to read particular document).
3) User can not read documents stored on other Users's cards even if s/he got physical access to memory of the card.
4) Department can not get access to another Department's documents that stored on the card (without granting special permission), even if it have physical access to memory of the card.
5) Department can not change User's documents without agreement of the User and User can not change his/her documents without agreement of the appropriate Department

Information security consists of the confidentiality, integrity and availability. [41] We can notice that five requirements described above provide security of stored at cards data. Data availability is ensured by properties 1 and 2, confidentiality provided by a combination of properties 3 and 4 and integrity is guaranteed by the property number 5. Therefore we can ensure, that in case when system satisfy five requirements it automatically meet requirements of information security.
We can make certain that current scheme fulfils requirements 1 – 5.

- Every User knows his/her own secret key and public keys of Departments. According to equation 4 User is able to generate encryption key and read all stored on card documents. It means that property number 1 holds.
- Every Department knows its own secret key and public keys of all users. It means that Department can decrypt

all files affiliated with it, and such process doesn't require any User interaction. In case when access rights were granted by other department secret key of Department issued the Document is known as well as User's public key, so the Document can be easily decrypted. According to this fact property number 2 is fulfils.

It is important to prove that keys generated by User and Department would be the same for the same document. We can prove a simple theorem:

Theorem 1. *Equation*

$$\begin{aligned} KEY_{k,i,j} &= UKey_{j,CC_k}^{DID_{i,CC_k}} \; mod \; c_k \\ &= DKey_{i,CC_k}^{UID_{j,CC_k}} \; mod \; c_k \end{aligned} \qquad (6)$$

holds for all i, j such that $i \in (1 \cdots M)$, $j \in (1 \cdots N)$ *where* M *is number of departments and* N *— number of users.*

Proof. Using equations 1 and 2 we can ensure that the both formulas for User and Department are equal to $a^{DID_{i,CC_k} \cdot UID_{j,CC_k}}$.

- We are able to decrypt file stored the card in two cases: when we know User's secret key and Depatrtment's public key or when we know User's public key and Department's secret key. User is not able to decrypt documents of other Users because s/he doesn't know neither secret keys of other Users nor secret keys of Departments even if s/he has physical access to card's memory. According to this consideration, property number 3 holds.
- As in previous case, Department is not able to decrypt documents of other Users because s/he doesn't know neither secret keys of Users nor secret keys of other Departments even if s/he has physical access to card's memory. According to this consideration, property number 4 holds.
- On the one hand, all documents stored on tags are signed by digital signature and every unauthorized modification violates the signature. On the other hand, User must bring his/her card to Department's terminal, so s/he will authorize changes by his/her actions. It means than property 5 holds.

From reasoning mentioned above we can conclude that both User and Department disable to access another's data without knowledge of User/Department secret key. The only way of getting such key is to generate it using corresponding public key and the Master Secret Key of Certification Center (a_k). It means that the only reasonable passive attack is one that aimed to find out a_k from secret key of User/Department and a couple of public keys of Users and Departments. This problem is very similar to discrete logarithm problem considered as hard [42]. Due to this fact the level of security for such system is high enough. However, Attacker can use Fermat's little theorem [47] in order to decrease complexity of the task. According to the theorem the following expression would be correct:

$$\left(a_k^{DID_{i,CC_k}}\right)^x = a_k \; mod \; c_k \qquad (7)$$

The Attacker has to find pair (x, t) such that

$$DID_{i,CC_k} \cdot x = t \cdot (c_k - 1) + 1 \qquad (8)$$

The only algorithm allows to solve this task is full search through all possible t that satisfy the following condition:

$$t \cdot (c_k - 1) + 1 = 0 \; mod \; DID_{i,CC_k} \qquad (9)$$

We can estimate the complexity of this attack as $c_k/6$, that is only 3 times lower than brute-force attack. It means that security level is appropriate. Besides, we developed an application which randomly selects a_k, c_k and $DID_{i,CC_k}$from more than 10 millions of primes and try to implement this search. Obtained results proved correctness of our evaluation. Based on facts mentioned above it can be noticed that for large c_k such type of attack in irrelevant. Active attacks are sophisticated due to small (up to 10 cm) range of NFC technology. User is able to notice any foreign objects in this range during authentication phase. Besides, such attacks are stumbling-stone of all wireless communication systems.

VII. Comparison with existing solutions

In Section II, we have classified the established approaches on user authentication to multiple information systems. According to this classification, the proposed scheme belongs to group 4a, i.e. it is a solution with a portable object of identifiers working in a non-interactive mode.

In this section, the qualitative comparison of our proposal with widely used solutions is presented. We focus primarily on the characteristics that are most important for the user. The following set of criteria is considered:

- *Battery.* Whether a battery on the key side is required.
- *CPU.* Whether computational power on the key side is required.
- *Size.* Physical size of the wireless key.
- *Complexity.* Computational complexity of the authentication algorithm.
- *Security.* Security level of the system.
- *Integrity.* Whether integrity is guaranteed.
- *Third-party.* Whether a trusted third party is involved.
- *Storage.* Where the sensitive information is stored: on the tag, IS or on the trusted third party.
- *PKI usage.* Role of Public Key Infrastructure (PKI) in the system: keys generation only; keys generation and granting/depriving access; keys generation, granting/depriving access and authentication, etc.
- *Deployment costs.* Estimation of the amount of changes in the infrastructure required to make the system operational.

We have selected a set of conventional authentication techniques that do not use wireless keys: Android 4.0 (and higher) login [24], Google Wallet [44], and fingerprint [45], as well as a number of popular authentication protocols, that are already applied to wireless keys or even could be applied in

TABLE I. QUALITATIVE COMPARISON OF DIFFERENT AUTHENTICATION TECHNIQUES

Solution	Battery	CPU	Size	Complexity	Security
Android 4.0 [24]	Not required	Not required	No device	Low	Low
Google Wallet [44]	Required	Required	Phone size	High	High
iOS Fingerprint [45]	Not required	Not required	No device	High	Low
OPACITY [34]	Required	Required	Phone size	High	High
EHLS [25]	Not required	Required	2 cm	High	High
LMAP [26]	Not required	Required	2 cm	Low	High
Our proposal	Not required	Not required	2 cm	Low	High

Solution	Integrity	Third–party	Storage	PKI usage	Deployment costs
Android 4.0 [24]	-	-	No storage	Not used	Low
Google Wallet [44]	+	+	Third-party	Auth.	Low
iOS Fingerprint [45]	-	-	Local	Not used	Average
OPACITY [34]	+	+	Local	Auth.	High
EHLS [25]	Partial	-	Local	Not used	Average
LMAP [26]	-	-	Local	Not used	Low
Our proposal	-	-	Local	Key gen. only	Low

theory: OPACITY [34], EHLS [25], and LMAP [26]. Results of comparison are presented in Table I.

We have compared the proposed solution with the representatives of the approaches described in Section II.

With respect to comparison results, presented in the table, our scheme reaches high level of security (see Section VI for details), while having much better reliability and deployment cost values. As such, we can claim that the authentication scheme, described in the paper, is beneficial for the commercial deployment, as well as the whole concept of wireless keys looks promising for the further research and improvements.

VIII. CONCLUSIONS AND DISCUSSION

In this paper, a novel wireless authentication key and secure documents storage for Internet of Everything was proposed. We suggest to use combination of strong cryptographic primitives to provide a proper security level. Offered solution doesn't require power on the Tag that makes it convenient for User. Besides, internet connection is not compulsory and all data stored not on remote database but on the User's tag. It leads to increasing the security level. One more benefit of the scheme is ability to share documents between Departments without enabling to change them illegally.

REFERENCES

[1] V. Petrov, "Feasibility study of the THz band for communications between wearable electronics," *In the Proceedings of the 17th Conference of Open Innovations Association FRUCT*, Yaroslavl, Russia, April 2015.

[2] A. Ometov, S. Andreev, A. Turlikov, and Y. Koucheryavy, "Characterizing the effect of packet losses in current WLAN Deployments," *In the Proceedings of the 13th International Conference on ITS Telecommunications (ITST), November 2013.*

[3] D. Evans, "The Internet of Things. How the Next Evolution of the Internet Is Changing Everything", *Cisco White Paper*, 2011.

[4] I. F. Akyildiz, M. Pierobon, S. Balasubramaniam and Y. Koucheryavy, "The Internet of Bio-NanoThings", *in IEEE Communication Magazine*, vol. 53, no'3, March 2015.

[5] A. Ometov, "Fairness characterization in contemporary IEEE 802.11 deployments with saturated traffic load," *In the Proc. of 15th Conference of Open Innovations Association FRUCT*, St Petersburg, Russia, April 2014.

[6] V. Petrov, S. Balasubramaniam, R. Lale, D. Moltchanov, P. Lio, Y. Koucheryavy, "Forward and Reverse Coding for Chromosome Transfer in Bacterial Nanonetworks", *in Nano Communication Networks (Elsevier)*, vol. 5, no. 1—2, March — June 2014.

[7] P. Boronin, V. Petrov, D. Moltchanov, Y. Koucheryavy, J.M. Jornet, "Capacity and Throughput Analysis of Nanoscale Machine Communication through Transparency Windows in the Terahertz Band," *Elsevier Journal on Nano Communications Networks*, vol. 5, pp. 72?82, September 2014.

[8] S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz, "Quantifying the security of graphical passwords: the case of android unlock patterns", *in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, ACM, pp. 161–172, 2013.

[9] Trusted Computing Group, "TPM 2.0 library specification", Web: http://www.trustedcomputinggroup.org/developers/trusted platform module/, 2013.

[10] V. Petrov, D. Moltchanov, S. Balasubramaniam, Y. Koucheryavy, "Incorporating Bacterial Properties for Plasmid Delivery in Nano Sensor Network", *in IEEE Transactions on Nanotechnology*, vol. 14, no. 4, pp. 751-760, July 2015.

[11] A. Pyattaev, J. Hosek, K. Johnsson, R. Krkos, M. Gerasimenko, P. Masek, A. Ometov, S. Andreev, Sergey J. Sedy, V. Novotny, and others, "3GPP LTE-Assisted Wi-Fi-Direct: Trial Implementation of Live D2D Technology," *ETRI Journal*, vol. 37, n.5, 2015.

[12] The Telegraph, "iPhone 5s fingerprint sensor 'hacked' within days of launch", Web: http://www.telegraph.co.uk/, 2013.

[13] V. Petrov, D. Moltchanov, Y. Koucheryavy, "Analytical Model of Link Reliability in Bacteria Nanonetworks," *1st ACM International Conference on Nanoscale Computing and Communication (ACM NANOCOM)*, Atlanta, GA, USA, May 2014.

[14] B. Schneier, *Applied Cryptography*, Second Edition, John Wiley & Sons, 1996.

[15] V. Petrov, S. Bezzateev, V. Zybin, "Wireless authentication using OPACITY protocol," *In the Proceedings of 7th International Congress on Ultra Modern Telecommunications and Control Systems (ICUMT)*, Brno, Czech Republic, October 2015.

[16] U. Uludag and A. K. Jain, "Attacks on Biometric Systems: A Case Study in Fingerprints", *in Proceedings of SPIE - The International Society for Optical Engineering*, 2014.

[17] FISP 197, "Advanced Encryption Standard", 2001.

[18] V. Petrov, D. Moltchanov, Y. Koucheryavy, "On the efficiency of spatial channel reuse in ultra-dense THz networks," *In the Proceedings of the IEEE Global Communications Conference (IEEE GLOBECOM)*, San Diego, CA, USA, December 2015.

[19] A. Ometov, K. Zhidanov, S. Bezzateev, R. Florea, S. Andreev, and Y. Koucheryavy, "Securing network-assisted direct communication: the case of unreliable cellular connectivity", *In the Proceedings of the Trustcom/BigDataSE/ISPA*, Helsinki, Finland, August 2015.

[20] V. Petrov, D. Moltchanov, Y. Koucheryavy, "Interference and SINR in Dense Terahertz Networks," *In the Proceedings of the IEEE 82nd Vehicular Technology Conference (IEEE VTC2015-Fall)*, Boston, MA, USA, September 2015.

[21] OpenID foundation, Web: openid.net, 2014.

[22] FISP 180-3, "Secure Hash Standard', 2008.

[23] D. Moltchanov, Y. Koucheryavy and J. Harju, "Performance response of wireless channels for quantitatively different loss and arrival statistics", *in Elsevier Performance Evaluation*, vol. 67, no. 1, pp. 1-27, 2010.

[24] S. Uellenbeck et al., "Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns", Web: https://www.hgi.rub.de, 2013.

[25] S.A. Weis, S.E. Sarma, R.L. Rivest, and D.W. Engels. "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", *In Proceedings of Security in Pervasive Computing* , vol. 2802 of LNCS, pp. 201 – 212, 2004.

[26] P. Peris-Lopez et al., "LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags", *workshop on RFID security (RFIDSEC06)*, 2006.

[27] FIDO Alliance Homepage, Web: http://www.fidoalliance.org/, 2013.

[28] F. Schaub, M. Walch, B. Könings, and M. Weber, "Exploring the design space of graphical passwords on smartphones", i*n Proceedings of the Ninth Symposium on Usable Privacy and Security*, ACM, p. 11, 2013.

[29] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey", *in Computer Security Applications Conference, 21st Annual* IEEE, 2005.

[30] D. Hardt, "The OAuth 2.0 authorization framework", 2012.

[31] A. Volkova, D. Moltchanov, V. Petrov, Y. Koucheryavy, "Joint Cooling and Information Transmission for Board-to-Board Communications," *In the Proceedings on the 2nd ACM International Conference on Nanoscale Computing and Communication (ACM NANOCOM)*, Boston, MA, USA, September 2015.

[32] J. Kohl and C. Neuman, "The Kerberos network authentication service (v5)", RFC 1510, Tech. Rep., 1993.

[33] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estévez-Tapiador, and A. Ribagorda, "LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags", *in Proceedings of 2nd Workshop on RFID Security*, p. 6, 2006.

[34] ActiveIDentity, "The Open Protocol for Access Control Identification and Ticketing with Privacy", Web: http://www.smartcardalliance.org/resources/pdf/OPACITY_Protocol-3-5-3.pdf, 2010.

[35] M. Gerasimenko, V. Petrov, O. Galinina, S. Andreev, Y. Koucheryavy, "Impact of machine-type communications on energy and delay performance of random access channel in LTE-advanced", *in European Transactions on Telecommunications*, vol. 24, no. 4, pp. 366–377, 2015.

[36] The Universal Electronic Card, Web: http://www.mos.ru/en/about/uec/, 2013.

[37] M. Gerasimenko, V. Petrov, O. Galinina, S. Andreev, Y. Koucheryavy, "Energy and delay analysis of LTE-Advanced RACH performance under MTC overload," *In the Proceedings of the 2nd International Workshop on Machine-to-Machine Communications - 'Key' to the Future Internet of Things at GLOBECOM'12*, Anaheim, CA, USA, December 2012.

[38] Coin Inc., OnlyCoin project, Web: https://onlycoin.com/, 2013.

[39] V. Petrov, S. Andreev, and Y. Koucheryavy, "An applicability assessment of IEEE 802.11 technology for machine-type communications", *in Proc. of the 11th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)*, Ayia Napa, Cyprus, 2012.

[40] S. Andreev, A. Larmo, M. Gerasimenko, V. Petrov, O. Galinina, T. Tirronen, J. Torsner, Y. Koucheryavy, "Efficient Small Data Access for Machine-Type Communications in LTE," *In the Proceedings of the IEEE International Conference on Communications (IEEE ICC)*, Budapest, Hungary, June 2013.

[41] Basic Information Security Principles Web: http://www.oregon.gov/DAS/CIO/ISRC/pages/intro_basics.aspx

[42] A. Menezes, P.C. Van Oorschot and S.A. Vanstone *Handbook of applied cryptography*, CRC Press, 1997.

[43] V. Petrov, S. Andreev, A. Turlikov, and Y. Koucheryavy, "On IEEE 802.16m Overload Control for Smart Grid Deployments", *in Proc. of the 12th International Conference on Next Generation Wired/Wireless Networking*, St. Petersburg, Russia, 2012.

[44] Google Inc., "Google Wallet", Web: http://wallet.google.com, 2012.

[45] Apple, "iPhone 5S Specification", Web: http://www.apple.com/iphone-5s/, 2013.

[46] V. Petrov, S. Edelev, M. Komar, and Y. Koucheryavy, "Towards the Era of Wireless Keys: How the IoT Can Change Authentication Paradigm", *in Proceedings of IEEE World Forum on Internet of Things*, Seoul, South Korea, March 2014.

[47] J. M. Cargal, *Discrete Mathematics for Neophytes: Number Theory, Probability, Algorithms, and Other Stuff*, JENNYMAC, 1988.