A Door Access Control System with Mobile Phones

Tomomi Yamasaki[1], Toru Nakamura[1], Kensuke Baba[2,3], and Hiroto Yasuura[2,3]

[1]Graduate School of Information Science and Electrical Engineering
[2]Faculty of Information Science and Electrical Engineering
[3]System LSI Research Center
Kyushu University
Motooka 744, Nishi-ku, Fukuoka, 819-0395, Japan
{yamasaki,toru,baba,yasuura}@c.csce.kyushu-u.ac.jp

Abstract. This paper proposes a door access control system with mobile phones which allows off-line delegations of an access. A model of door access control with mobile phones is introduced, and then the delegation is formalized as a copy of a door-key. On the previous model, secure copy by off-line is realized using the essential idea of the proxy signature. Moreover, the proposed system is implemented on mobile phones, and then the execution time of a copy and a verification are estimated. As a result, it is shown that the proposed system is feasible.

Keywords: Access control, door-key management, mobile phone, off-line delegation

1 Introduction

Service providing systems using portable devices, for example, a door access control system with smart cards, are being popular in our daily life. In most of such systems, the scheme to control authorities to receive a service is based on entity authentications (or identifications) by communications with electronic data, and therefore the portable device stores secret information for the identification. In this sense, the portable device (such as a smart card, a PDA, a mobile phone, and so on) is called a "token".

In some practical systems providing a service, a delegation of the authority for a service can be a very useful function. For example, in a door access control system, copying a door-key may be the most common requirement. In an authority management system with token based identifications, passing the token is the naive scheme to realize a delegation, however it is not practical if the token is for multiple services. Therefore, the scheme based on cryptographic technologies with passing only electronic data is necessary to meet the requirement. In this approach, a delegation is straightforwardly realized if we allow a communication with the entity who manages the authorities. However, it is not clear how to realize an off-line delegation, that is, a delegation without any communication with the third party.

Please use the following format when citing this chapter:

Yamasaki, T., Nakamura, T., Baba, K., Yasuura, H., 2007, in IFIP International Federation for Information Processing, Volume 245, Personal Wireless Communications, eds. Simak, B., Bestak, R., Kozowska, E., (Boston: Springer), pp. 230-240.

We consider the situation that an entity who has an authority (hereinafter called an "owner") wants to delegate the authority to other entity (hereinafter called a "deputy"). The idea of proxy signature [4, 3] can be a method to realize a off-line delegation of an authority. The entity creates the signature for the public-key of the deputy, and the owner sends the digital signature to the deputy as a warrant. The deputy sends the warrant to the verifier with the deputy's signature. Similar methods can be found in systems of electronic cash [6, 1]. The idea of "transferability" corresponds to the off-line delegation. A user issues the license from the bank. The user issues electronic cash from the bank by using the license, and use cash for the settlement in the retail store. When an owner delegate it to a deputy, the owner sends a certification which denotes the delegation. Although there are many of related work about the protocol of the authority delegation, applying the ideas to a practical system needs more discussion. This difficulty depends on at least the following two factors:

- the difficulty of modeling practical systems which manages authorities,
- the gap between the ideal environment required from the theoretical schemes and the current technologies.

This paper focuses a door access control system and proposes a technique for applying the essential idea of the proxy signature to the authority delegation. First, we introduce a model of door access control to make clear the requirements of practical systems. If we consider the delegation of a door-key, we can ignore a double-use of the authority in most case. This is a critical difficulty for the transferability of electronic cash. Using mobile phones solves the second factor of the previous difficulty, since the input devices and the screen which displays the result of the data exchange are provided. Moreover, some kinds of mobile phones have the infrared rays communication function and the integrated circuit chip [5], while the intercommunication function is not provided in smart card. The mobile phone possesses the input function and the screen, therefore it is suitable for exchanging data. Then, we have the following assumptions on our model:

- the delegation allows a double use of the authority,
- an owner and a deputy can have secure communication without any third party.

Even on the strong assumptions, it is not trivial to realize the off-line delegation. Our scheme is a simple application of the idea of an encryption or an digital signature technology. Moreover, we implement our scheme on practical mobile phones and evaluate the feasibility.

This paper is constructed as follows: in Section 2, we describe some requirements of door access control systems with mobile phone from a practical viewpoint; in Section 3, we introduce a model of door access control and interpret the requirements to the model, and then propose a scheme to control authorities which allows off-line delegations; in Section 4, we show the environment and experimental results of the implementation of the proposed scheme.

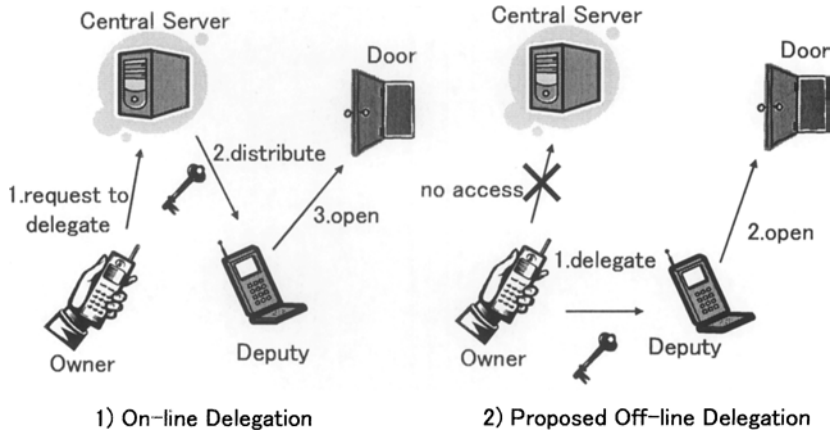

Fig. 1. On-line and off-line delegations

2 Requirements of Door Access Control Systems

In this section, we show effective application examples of a door access control system we are considering, and describe some requirements from two viewpoints. Fig. 1 shows the outline of our system.

2.1 Examples of Practical Use

Temporal Delegation When we consider a door-key, for example, of our private room, our office room, a public conference room, and so on, it often happens the case that we want to lent the door-key to our friend, colleagues, students, and so on. In the case of a physical door-key, we must lent our master key itself or a copied one. It is easy to imagine insecure or uneconomic situations. These problems can be solved by electronic keys with detailed information about the key such as a restriction of doors or time for use. If we use a portable device such as a smart card for the electronic key, the authority control is important especially for a multi-services system. Do you want to lent your smart card with a credit service to let your student use a conference room?

Load Distribution An off-line delegation key management system can provide better performance than on-line, from the viewpoint of reducing their burdens to change key management databases on an central server. In on-line system, the central server must change the database every time when a user asks the server to delegate his/her key to others. On the other hand, in off-line system, a user can delegate his/her key without access to the central server. Additionally an off-line delegation realizes a hierarchical manage of user's keys. For example,

in the case where a boss tries to manage 1,000 keys for 100 company members, the boss just has to delegate 100 keys to 10 general managers of him and change his database for only the part with respect to the managers.

2.2 Information as a Door-key

The identification between the server and a user is well studied and there exist schemes which are secure in a practical sense for the situation that the communicating entities have computing resources. Especially, the identification of the server by any user is straightforward in the case that the server is regarded as an entity connected to a door.

If we consider the delegation of a door-key, we can ignore a double-use of the authority, since in most case the service for the authority does not disappear by a use. Therefore, we can consider as a delegation of an authority a copy rather than the delegation in the strict sense.

In some application of a door access control system, the authority is delegated for free as the examples in this section. In such cases, it is not necessary to confirm that a delegated door-key is the correct one. Therefore, we can use a simple scheme of a delegation and a verification of an authority. If the confirmation is necessary, an idea of the digital signature is used instead of a private-key encryption.

2.3 Communication between Mobile Phones

Although the intercommunication function is not provided between smart cards, there exist some kinds of mobile phones which have an infrared communication function [5]. Therefore, we can allow as processes of a door-key not only the communication between a server and a user but also two users. This is the essential technology to realize an off-line communication.

Some mobile phones have also enough resource for computations of encryption, and therefore we can assume an ideal identification between users. Moreover, the following two considerations show an appropriateness of the previous assumption: 1) we usually face to the other entity when we use a mobile phone to send data, hence we can identify the entity in the sense of a real communication rather than electronic process; 2) we carry our mobile phone all the time, hence the correspondence between a human and his/her mobile phone is guaranteed.

3 Formalization

In this section, we introduce a model of a door access control system with mobile phones and interpret the requirements in the previous section to the model. Then, we propose a scheme of a verification and a delegation of the authority to open a door.

3.1 Door Access Control System

A *door access control system* is constructed by *users* who want to use their authority to open a door and a *server* who examines whether a user has the authority. We denote by $u_1, u_2, \ldots \in U$ the users and by s the server. Any $u_i \in U$ and s can communicate another entity along with a given protocol. By the argument in Subsection 2.2, we formalize this protocol that a $u_i \in U$ submit a string to s to open a door, and s outputs whether the u_i has the authority. We call this process a *verification* by s of u_i with respect to a door. In the rest of this paper, we consider a door access control system with a single server in the situation that the server controls a single door, and therefore we regard the server and the door as a single entity.

For the previous model, we allow some process between two users. Any $u_i \in U$ can operate interactive processes with another $u_j \in U$ along a given protocol, which is reasonable for systems with mobile phones by the argument in Subsection 2.3. Additionally, by the argument, we assume an ideal identification between any two entities in the users and the server, which enable any user to confirm the identifier, called the *ID*, of the other user.

Assumption 1 *Any pair of entities in $U \cup \{s\}$ has a scheme of an identification.*

By the previous assumption, any entity can know the ID of the other entity. The ID of a user u_i is denoted by n_i. In some protocols in the rest of this paper, the identification process is not described explicitly. Note that the ideal identification is not realized by the ID, but the ID is confirmed as the result of the identification. It is not in the scope of this paper how to realize a secure identification.

As mentioned in the argument of the previous assumption, we assume any pair of communicating entities can use a suitable cryptographic technology, since the system is realized by a server computer and mobile phones which have enough resource for computations. We consider the following two conditions.

Assumption 2 *Each user in U and s have a private-key encryption scheme, respectively.*

By the previous assumption, u_i has a function ϕ_{u_i} for an encryption and s can know (the result of an application of) $\phi_{u_i}^{-1}$. The condition also yields that any user has a scheme of a message authentication code to s, that is, s can verify the data integrity of the message from the user [2].

Assumption 3 *Any entities in $U \cup \{s\}$ has a public-key encryption scheme.*

By the previous assumption, any entity in $U \cup \{s\}$ has a scheme of a digital signature [2]. In addition to the situation by Assumption 2, this condition yields that any entity can verify the integrity of a message with the digital signature from any user.

3.2 Copy of an Authority

We introduce an idea of "trust" on a door access control system. The ideal assignment of the authority to open a door to the users is expressed by a function $F : U \to \{0, 1\}$ such that $F(u_i)$ is 1 if u_i should have the authority, and 0 otherwise. Now we consider a door access control system Σ in which any verification by s terminates for any user in U. Then, the result of practical verifications in Σ is also expressed by a function $G_\Sigma : U \to \{0, 1\}$ such that $G_\Sigma(u_i)$ is 1 if the verification outputs that u_i has the authority, and 0 otherwise. A door access control system Σ is *trustful* if, for any u_i, $G_\Sigma(u_i) = 1$ if and only if $F(u_i) = 1$.

Let Σ be a door access control system such that $G_\Sigma(u_i) = 1$ and $G_\Sigma(u_j) = 0$ for $u_i, u_j \in U$. Then, a *copy of the authority* is a process to change Σ into Σ' such that $G_{\Sigma'}(u_j) = 1$ and $G_{\Sigma'}(u_k) = G_\Sigma(u_k)$ for the other $u_k \in U$. Therefore, the ideal assignment $F' : U \to \{0, 1\}$ after the copy to u_j is

- $F'(u_k) = 1$ if $F(u_k) = 1$ or $u_k = u_j$,
- $F'(u_k) = 0$ otherwise.

We denote the ideal assignment F' of the authority after a copy from u_i to u_j by $F \cup f_{u_i \to u_j} : U \to \{0, 1\}$. The previous notation can be extended straightforwardly to the ideal assignment after plural copies with a suitable definition of $\cup$. Then, in the followed subsection, we show that the system after a copy operated by our scheme is still trustful.

Note: By allowing the copy of the authority, a part of the access control is entrusted to the users who has the authority. If we express by $F_s : U \to \{0, 1\}$ the assignment of the authority by s on an initial condition, and by $F_{u_i} : U \to \{0, 1\}$ u_i's will whether he/she wish to copy his/her authority to each user, then the ideal assignment $F_s \cup F_{u_i} : U \to \{0, 1\}$ can be defined as

- $F_s \cup F_{u_i}(u_k) = 1$ if $F(u_k) = 1$ or there exists $u_i \in U$ such that $F_s(u_i) = F_{u_i}(u_k) = 1$,
- $F_s \cup F_{u_i}(u_k) = 0$ otherwise.

Since a mapping from a set to $\{0, 1\}$ is defining a subset of the set, it is easy to extend our idea with this expression to more complex controls, for example, authorization with recommendations by plural authorized users.

3.3 Procedures

As we mentioned in this section, the basic protocol of the verification of the authority is a submission of a string by a user to the server after the identification between the two entities. The string submitted in the protocol is called a *door-key* and denoted by K. Then, we show the procedures to verify or copy a door-key.

By Assumption 1, if we consider a system in which any copy of the authority is not allowed, then it is trivial that a trustful system can be realized by the ideal identification of $u_i \in U$ by s. s has only to prepare the function of the ideal

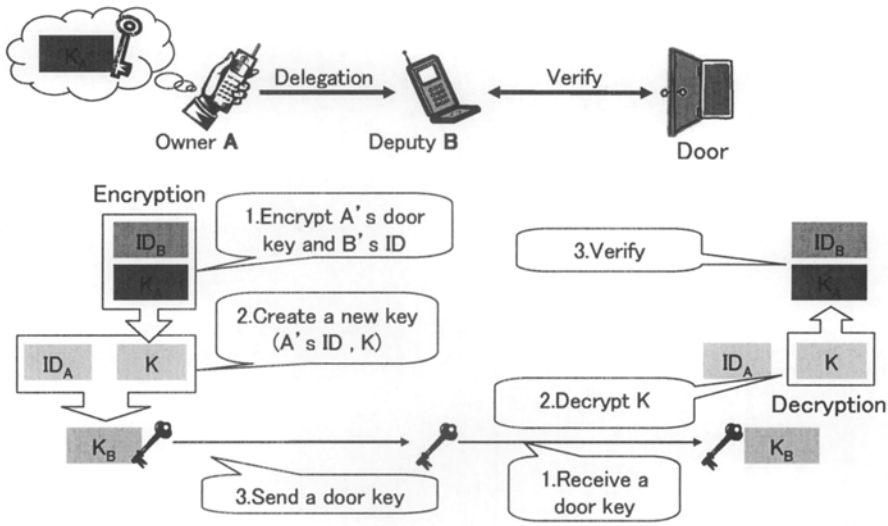

Fig. 2. Overview of the proposed delegation scheme.

assignment of the authority to the users. It is also trivial that an on-line copy, that is, a copy by modifying the function for every copy yields a trustful system. We consider a system with off-line copies. The outline of the proposed system is illustrated in Fig. 2.

Consider a copy of an authority from u_i to u_j. The following is the procedure of u_i after the identification between u_i and u_j, where ϕ is a function for encryption.

Procedure 1 (copy) *u_i submits $K = (n_i, \phi_{u_i}(n_j))$ to u_j.*

Then, the following is the procedure of the verification by s of u_j. Before the procedure, s and u_j operate the identification and u_j submit K which is copied from u_i along the previous procedure. Let $K[i]$ be the ith element of K.

Procedure 2 (verify) *s outputs*

- 1 *if* $F(u_j) = 1$,
- 0 *if* $F(u_j) = 0$ *and* $F(u_i) = 0$,
- 1 *if* $F(u_i) = 1$ *and* $\phi_{u_i}^{-1}(K[2]) = n_j$,
- 0 *otherwise.*

In the previous procedure, the first step is same as the procedure for a system does not allow any copy. The second and third step correspond to the ideal assignment after the copy from u_i to u_j. Therefore, a criterion of trust of the system depends on ϕ, in other words, this system is trustful if ϕ is ideal. In the system with Assumption 2, the entity who receive the door-key by a copy cannot

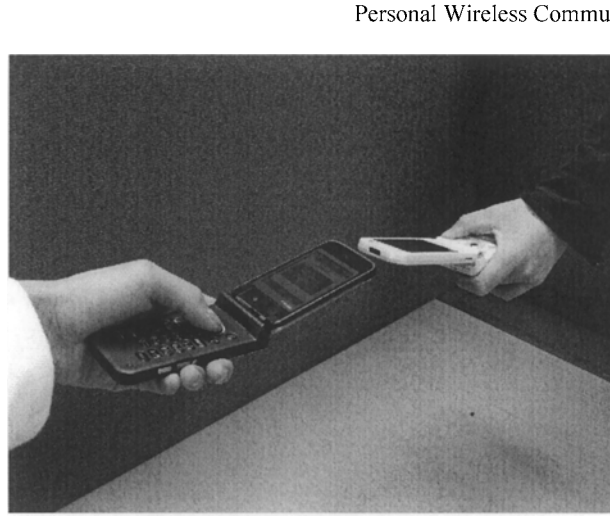

Fig. 3. An infrared communication between mobile phones

confirm the door-key is correct. Therefore, the entity who copy the door-key can success an attack to get a compensation for the door-key. In a practical sense, this situation is not fatal in some cases, as we mentioned in Subsection 2.2. In the system with Assumption 3, the attack is prevented since any user can confirm the door-key. In this case, some messages which describes what K is are submitted with K.

Note: We can easily extend the system to allow recursive copies by applying ϕ to K in Procedure 1. Then, Procedure 2 is modified to repeat the second and third step till the ID of the communicating entity appears. In this case, the length of K depends on the depth of the "sublease", and hence a restriction of the number of copies or a synchronization with the server for a period is required.

4 Implementation

In this section, firstly, we show the implementation environment. Secondly, we show the experimental result of the proposed system in this environment. Finally, we discuss the feasibility and usefulness of the proposed system.

4.1 Environment

We implement the idea in the previous section into a mobile phone which has a infrared communication function (see Fig. 3) and a contactless IC chip [5]. Table 1 shows the execution environments of the mobile phone and the server in this implementation.

At the present time, in mobile phones which is usualy avairable, there is no cryptographic co-processor which can be used freely. Moreover, any significant

Table 1. The environment of our implementation

Device	Model	NTT DoCoMo F902i and F902iS
	OS	Symbian OS
	CPU	SH-Mobile
	Bandwidth of infrared communication	max 100 Kilo-Bytes
	IC chip	FeliCa chip (64 Bytes memory)
R/W	Model	RC-S440C
Server	OS	Microsoft Windows XP
	CPU	Pentium4 3.20GHz
	RAM	2.00GB

cryptographic algorithm implemented as a software can not execute in a practical time due to the poor resource of a mobile phone. Therefore, we estimate the execution time for the cryptographic algorithm from the result of another experiment on an JAVA card. In the implementation for mobile phones, we use an exclusive-or operation as a dummy cryptographic function with the user's identifier and secret information of length 4 bytes, respectively.

We consider the situation that a user u_i copies his/her door-key K to another user u_j, and the server s verifies u_j' authority. Let σ_i be the u_i's secret and rw the Felica chip Reader/Writer. Then, the protocols of a copy and verification of a door-key are as follows, where $\oplus$ denotes the bitwise exclusive-or.

Copy-Protocol:

STEP1: u_i calculates $K = (n_i, n_j \oplus \sigma_i)$;
STEP2: u_i submits K to u_j by using the infrared communication function;
STEP3: u_i writes K to the access area of u_j's IC chip.

Verify-Protocol:

STEP1: rw waits for accession u_j with polling;
STEP2: rw reads K from u_j's access area;
STEP3: rw sends K to s;
STEP4: s verifies K and σ_j.

4.2 Evaluation

We measured the execution time of the previous protocols on mobile phones and a server. Each execution time is conducted as the average of 10 trials. In Copy-Protocol, the process consists of three parts: generating K, an infrared communication, and writing K on an IC chip. In Verify-Protocol, the process consists of three parts: reading K from an IC chip, a radio communication (including a PIN authentication), and a verifying K. The experimental results of the execution time are shown in Table 2.

Table 2. The experimental results of the execution times

Protocol	Operation	Execution time (sec)
Copy	Generating K	0.002
	Infrared communication	3.302
	Writing K	0.690
	Total	3.994
Verify	PIN authentication	0.112
	Reading K	0.036
	Verifying K	0.002
	Total	0.150

4.3 Discussion

According to the result with respect to Copy-Protocol, the execution time of the infrared communication occupies a large portion of the total time. As we mentioned, in the step of generating K, an exclusive-or operation is used in place of a complex cryptographic function. Therefore, we measure the execution time of the cryptographic part on a smart card and estimate the time on a mobile phone.

Some smart cards have a cryptographic co-processor which can be used freely. Mobile phones will have the same cryptographic co-processor as smart cards since mobile phones with an IC chip can use for the usage to a smart card. Therefore, as another experiment, we measured the execution times of DES and RSA on JAVA Card to estimate the performance of mobile phones. In the experiment by JAVA card, the execution time of DES and RSA are 0.05 seconds and 0.21 seconds, respectively. The times are short compared with the execution times of an infrared communication and writing K on an IC chip. Thus, the gap between the execution times on a mobile for DES/RSA and the exclusive-or operation seems not to lead fatal inconsistency on our implementation.

As to the result for Verify-Protocol, the execution time of the PIN authentication occupies a large portion of the total time. Supposing that we adopt an advanced cryptographic function, the time for the verifying K will be longer. We can expect that the influence for the total execution time is small, since server has a lot of resources.

From the previous discussions, we can show that mobile phones can unite practicable operation time and safety in the future as adopted our proposed system.

5 Conclusion

We proposed a door access control system with mobile phones which allows off-line copies of a door-key. A model of door access control with mobile phones was introduced, and then a copy of a door-key and a criterion of security were formalized. On this model, a secure copy by off-line was realized using the essential

idea of the proxy signature. Moreover, the proposed system was implemented on mobile phones.

Acknowledgment

This work has been supported partially by the Grant-in-Aid for Scientific Research No. 17700020 of the Ministry of Education, Culture, Sports, Science and Technology (MEXT) from 2005 to 2007.

References

1. T. Eng and T. Okamoto. Single-term divisible electronic coins. In *Proceedings of EUROCRYPT' 94*, volume 950, 1994.
2. O. Goldreich. *Foundations of Cryptography.* Cambridge, 2001.
3. M. Mambo, K. Usuda, and E. Okamoto. Proxy signatures: Delegation of the power to sign messages. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E79-A(9):1338–1354, 9 1996.
4. B. Neuman. Proxy-based authorization and accounting for distributed systems. In *Distributed Computing Systems, 1993., Proceedings the 13th International Conference on*, 1993.
5. NTT DoCoMo Inc. http://www.nttdocomo.com/.
6. T. Okamoto and K. Ohta. Universal electronic cash. In *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, volume 576. Springer-Verlag, 1991.