IEEE Copyright Notice

© 2008 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

A Study on User Authentication Infrastructure for Next Generation Telematics

Katsuyuki Umezawa, Seiichi Susaki, Masamori Kashiyama and Satoru Tezuka

***Abstract*— To receive a telematics service, it must first be authenticated, and each automobile (or car navigation system) has typically been linked to a particular vehicle owner who could authenticate such services. However, an increasing number of drivers use cars that are rented, leased, or obtained through a car-sharing program; in such cases, the present form of car authentication is insufficient. A better system would authenticate the individual who is using a car at a particular time, but is not necessarily the owner. In this paper, we propose a personal authentication infrastructure for next-generation telematics. Specifically, we propose personal authentication into that (1) between the person and the terminal, (2) between the terminal and the center.**

I. INTRODUCTION

The use of car navigation systems and personal navigation devices (PNDs) has spread rapidly, and this has been accompanied by development of high-speed, wireless communication infrastructure such as that based on WiMAX. In such an environment, a car navigation system connects to a network to receive various services. However, before a service is provided, it is necessary to confirm whether a user requesting the service has the right to receive that service.

In the past, each car was typically owned by one person, and the person who used the car was generally fixed. In such a situation, the service provider only had to authenticate the car or the car navigation system, and for this hardware-based authentication is sufficient. However, common forms of car usage have changed, meaning that each driver can no longer be consistently linked to a single vehicle, and hardware-based authentication is no longer adequate.

In this paper, we consider changes in the environment that surrounds a car, and propose a user authentication mechanism that will better meet the needs of car users in the future.

In Section 2, we explain how the environment that surrounds a moving vehicle has changed. We describe the authentication infrastructure requirements for next-generation telematics in Section 3. In terms of those requirements, we describe the proposed authentication technique for telematics in Section 4. Specifically, we categorize personal authentication into that (1) between the person and the terminal, (2) between the terminal and the center, and (3) between the terminal and the service provider (ASP), and propose a method for No.(1) and No.(2) authentication category. We briefly discuss the application of our method in Section 5, and conclude in Section 6.

K. Umezawa, S. Susaki and M. Kashiyama are with Hitachi, Ltd.
S. Tezuka is with Hitachi Consulting Co., Ltd.

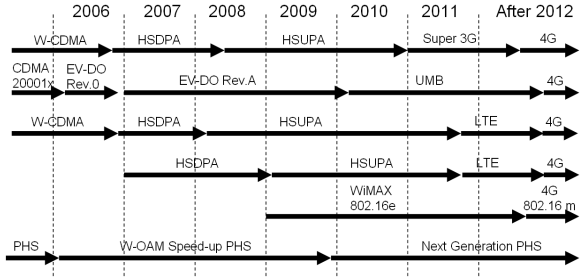

Fig. 1. Road Map of Communication Environment

II. CHANGE OF ENVIRONMENT

First, we will explain how the telecommunication environment that surrounds a vehicle in operation has changed in recent years.

A. Change of Communication Environment

A road map of the changes in Japan's telecommunication environment is shown in Fig. 1. As illustrated, the broadband environment has become faster and more extensive through advances in telecommunication technology.

B. Change in Navigation Terminals

The sales of navigation systems have steadily expanded in Japan's domestic market, and foreign markets have also grown rapidly, especially through sales of personal navigation devices (PNDs).

C. Changes in Service Style

Consider for a moment, the development of cellular phone services in Japan. Several years ago, cellular phone users could only connect to an official service provider via a portal site that a mobile carrier had prepared. In addition, a mobile carrier rather than the service provider collected the contents charge. However, as many general sites became available, the user could reach these sites through a general search site, and the number of service providers who collect charges directly has increased rapidly.

In such a situation, we can easily imagine that telematics services will be open services. In a word, they will be globalized and a variety of service providers will appear to provide these services; this is in contrast to the current situation where each car company provides its own special services. The concept of the globalization of service is illustrated in Fig. 2.

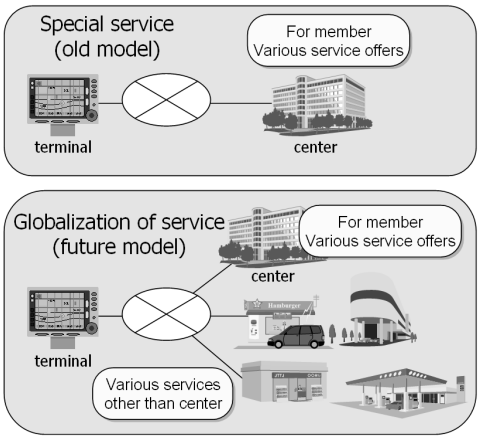

Fig. 2. Globalization of Services

D. Change in User Attitudes towards Car Ownership

The desire to own a car has lessened in Japan, especially among young people. Many people are now satisfied with renting a car when one is needed, for example for weekend activities. In addition, many drivers prefer to lease a car so that they can regularly switch to a newer model. Car-sharing programs, where two or more users share each car, is also becoming more common.

TABLE I shows the potential person:car (i.e., car navigation system) relationships depending on the different forms of car ownership and use.

TABLE I
CAR USE STYLE

#	Navi. : Person	Example
1	1:1	Personal use
2	1:m	Company car, Family use
3	n:1	Private car + Rental car, Change of lease car
4	n:m	The above combinations and car sharing

Service provision will have to correspond to “n:1” or “n:m” relationships in the future, rather than only the “1:1” or “1:m” relationships that have been accommodated up to now. This means that hardware-based authentication will no longer be sufficient, and user authentication will be required.

III. AUTHENTICATION INFRASTRUCTURE REQUIREMENTS

As the communication environment that surrounds the car continues to become faster and more extensive, the car is increasingly likely to be connected to the network without interruption. Given this assumption, there are two requirements that must be met to enable the globalization of service and personal authentication. In addition, any proposed method should be a technology that is applicable worldwide rather than only in Japan.

In Fig. 3, we show an image of a future user-authentication system that surrounds the car based on these requirements.

IV. PROPOSED USER AUTHENTICATION INFRASTRUCTURE FOR TELEMATICS

We will now explain our proposed personal authentication base for telematics that will enable user management based on the individual. We achieve this by managing the user as an individual, rather than as a user based on the car (car navigation system. In addition, this enables management of each user who uses a lease/rental car.

We apply the PKI authentication method based on public key cryptosystem technology as a personal authentication method and combine this with the current method of using an ID/Password. The advantages of using the PKI authentication method for telematics are listed below.

- The PKI technology is more secure than ID/Password since no confidential information flows through the network.
- Not much confidential information (passwords) of members has to be safely managed at the center. There is less danger of information leakage, and a slimmer center is practical.
- Unification of the user authentication among service providers other than the center is enabled. The ID/password need not be disbursed to each service provider, and the user need not remember many different ID/passwords.

Moreover, to achieve personal authentication rather than car authentication, we propose an authentication method with a secure device (an IC card, cellular phone, etc.) that the user possesses. Authentication with a secure device for telematics has the following two advantages.

- Correspondence between the terminal and globalization is enabled. That is, managing each user’s confidential information with a device that can be easily carried by the user allows the information to correspond to various terminals (navigation systems, PCs, smart phones, etc.) and scenarios (rental user, etc.)
- User-based rather than hardware-based authentication is enabled. The individual driving a car can be authenticated using a cellular phone and IC card; i.e., an individual ownership device and an authentication device.

A. Outline of proposed system

Figure 4 shows an outline of the proposed system.

The center side system is composed of two hierarchies in which it is considered to attest the car user in not only Japan but also the world, and puts subordinate position certification authority (CA) of each region in the world on the subordinate of route CA. These CA issues a digital certificate to the user in each country. In addition, at run time, a certificate verification server (CVS) that has a fast verification algorithm does the verification processing of a digital certificate. The center also has a coordinated authentication (single sign-on) function with the service provider.

To explain how our method is applied, it is useful to separately examine the authentication (1) between the terminal and the center, (2) between the center and the service

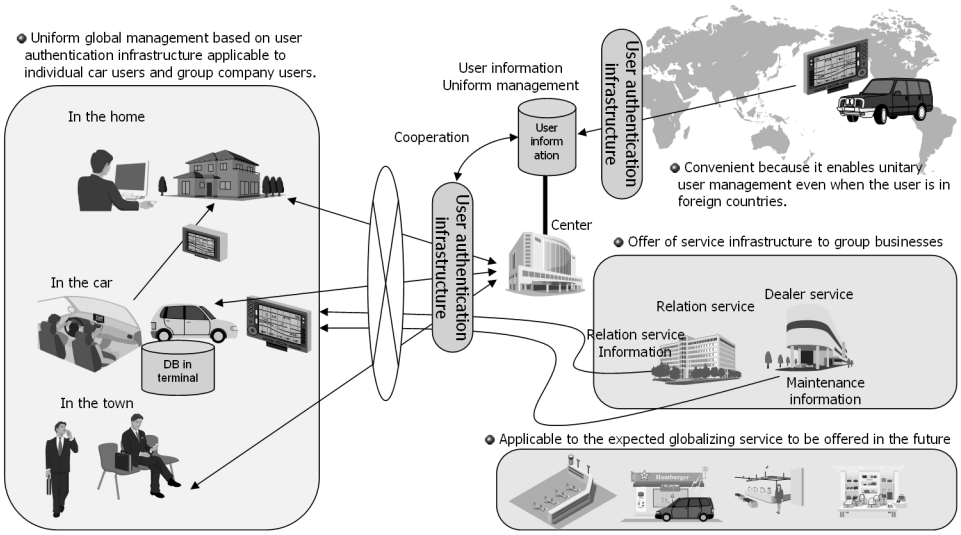

Fig. 3. Future world

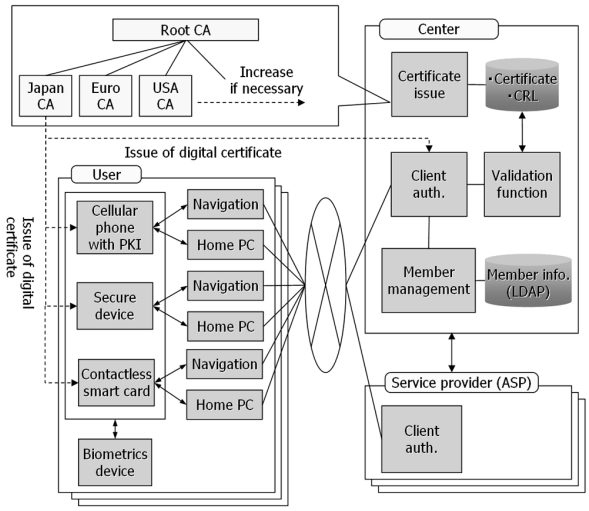

Fig. 4. Configuration of proposed system

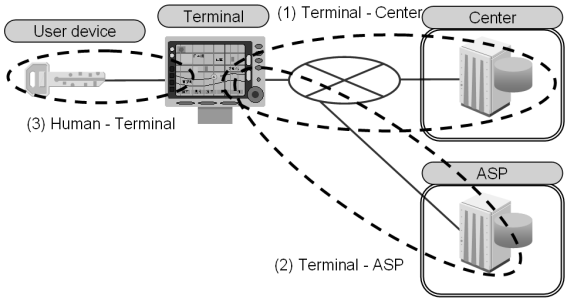

Fig. 5. Object of consideration

provider (ASP), and (3) between the person and the terminal, so that we may describe the composition of the system's authentication infrastructure and how the method works in each phase.

(1) Between the terminal and the center

We propose two kinds of ID/Password method and PKI method based on the public key cryptosystem technology as the authentication method between the terminal and the center [1].

- ID/Password technology.
- PKI technology.

(2) Between the center and the service provider(ASP)

The single sign-on function is necessary to achieve seamless access between the terminal and two or more ASPs. The method to enable single sign-on incorporates the following three methods.

- Method of connecting directly with ASP ("Direct Model")
- Method where the center mediates ("Center Mediation Model")
- Method of communicating directly with ASP after center provides authentication ("Integrated Model")

(3) Between the person(user device) and the terminal

We propose the following six methods as candidates for the user side device.

- The user selects from a menu (the device is not used).
- RFID device (smart key, etc.)
- Contactless Smart Card
- Cellular phone (NFC interface)
- Cellular phone (Bluetooth interface)
- Biometrics device(finger vein)

In this paper, we describe above-mentioned No.(1) and No.(3).

[1]One-time password methods and so on are candidates, but are unsuitable for telematics authentication because it is necessary to input a password that is updated over time.

B. Proposed method between terminal and center

The conventional composition and the proposed composition of the center side system are compared in Fig. 6.

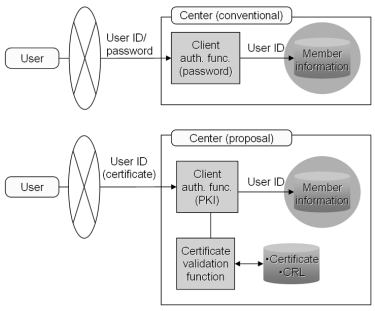

Fig. 6. Conventional and proposal configuration of center system

A conventional system authenticates the car as shown in Fig. 6 through transmission of an ID/password or equipment information such that relating to the car navigation system. The proposed system authenticates a person by transmitting a digital certificate [2]. The client authentication function in the center receives a digital certificate, and verifies that it has not lapsed, that the expiration date has not passed, etc.

C. Proposed method between device user and terminal

1) Method to use a cellular phone as an authentication device: We previously reported on our development of an authentication infrastructure system that uses the cellular phone [1][2][3][4][5][6]. These reports describe the certificate validation model and a certificate validation system that considers the restrictions unique to a mobile terminal. Evaluations have shown that this system enables secure mutual authentication between a cellular phone and an ASP.

We propose applying this authentication infrastructure system with a cellular phone terminal for telematics. Figure 7 shows an outline of our method to use the cellular phone as an authentication device.

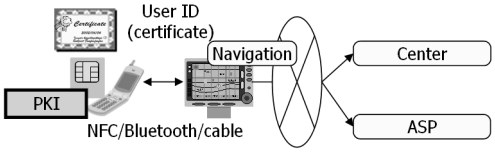

Fig. 7. Use of a cellular phone as an authentication device

As shown in Fig. 7, an digital certificate is stored in the UIM chip in the cellular phone in this method, and the cellular phone connects to the car navigation system terminal by NFC, Bluetooth, or cable. The car navigation system does the signature generation in UIM in response to the authentication request (challenge) from the center. The center authenticates the user by confirming a digital certificate and the signature value.

Given how widely cellular phones are now owned, this will be a convenient approach for users.

2) Use of a secure device as an authentication device: A secure device (KeyMobile) card is a card with an IC chip function and a memory card function, and it is used by inserting it into a memory card slot. Figure 8 shows the internal composition of a KeyMobile Card.

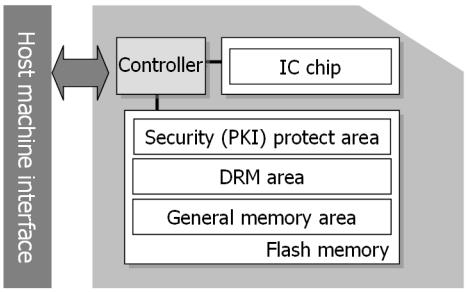

Fig. 8. KeyMobile Card

The notable characteristics of the IC chip are

- a Card OS for multiple applications
- conforms to the GlobalPlatform^{TM} specification (open platform specification for multifunctional smart cards)
- standard equipment for PKI technology.

We propose applying this KeyMobile Card to the authentication infrastructure for telematics. Figure 9 shows an outline of the method to use the KeyMobile Card as an authentication device.

As well as with car navigation systems, the KeyMobile Card can be conveniently used as an authentication device with other terminals, with the advantage that the map data and so on can be carried as bridge media since memory card slots have already been installed in various information.

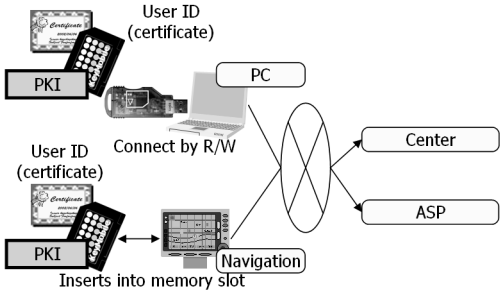

Fig. 9. Use of a secure device as an authentication device

3) Use of a contactless smart card as an authentication device: We also developed a method to use the contactless smart card that is convenient for users.

It is necessary to authenticate the server to receive service through a general ASP. However, when a contactless smart card is used, it is difficult to end the server authentication processing including the network delay. To deal with this

[2]More specifically, the center transmits a challenge (random numbers), the terminal generates a signature for the random numbers with a private key maintained in the secure device, and then the terminal transmits an electronic certificate and a signature value to the center.

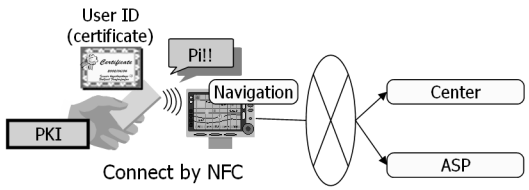

Fig. 10. Use of a contactless smart card as an authentication device

problem, we developed a method of mutual authentication, including the server authentication, even when a contactless smart card is used. Figure 11 shows the proposed flow. Thus, the user does not to have to wait for a response from a server that keeps holding up the contactless smart card because the car navigation system authenticates the server instead of the contactless smart card. As a result, the authentication method combined with the safety of the cross certification based on PKI is more convenient for a user who momentarily ends processing by not making contact.

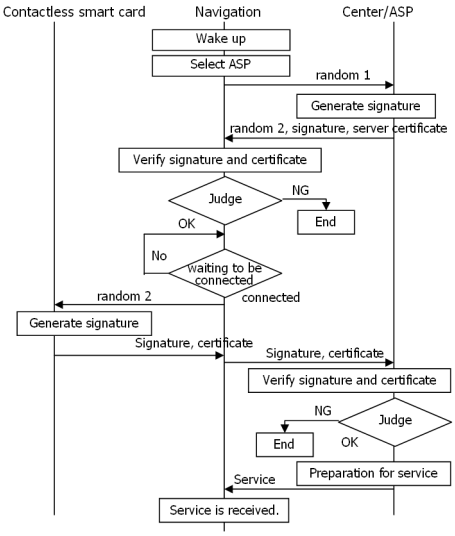

Fig. 11. Basic flow of method using contactless smart card device

4) Use of a biometrics device as an authentication device: Use of a biometrics device could further enhance the user's convenience. Figure 12 outlines our method to use a biometrics device as an authentication device.

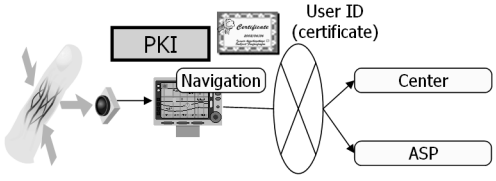

Fig. 12. Use of a biometrics device as an authentication device

The individual is specified by setting up a biometrics information reader in a part of the car that the driver normally touches, such as the steering wheel. However, some problems related to the matching of biometrics information on the server side still need to be resolved; for instance, matching speed decreases when the number of users increases, the potential leakage of biometrics information is a security concern, and the size of the center system will probably have to increase when using it in combination with other methods [3].

5) Method to select ID/password: Figure 13 shows an outline of the method to select an ID/password by touching the display with a finger. In this method, all ID/password for the driver is registered beforehand in the car navigation system. When the user starts to drive, he can select himself as the car driver from the menu and the preregistered ID/password is then transmitted to the center. This method is less secure than the PKI method, but such a system will be less expensive to manufacture. Moreover, registration is needed for use with a rented car.

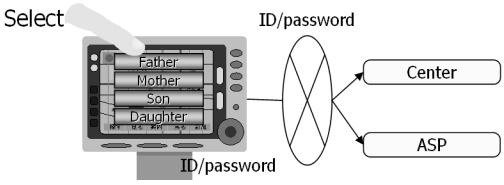

Fig. 13. Manually selecting from a menu

6) Selecting an ID/password with an RFID device: Figure 14 illustrates the method to select an ID/password using an RFID device that the user owns rather than manually selecting as described above. This should be more convenient for the user. However, it will be necessary to prevent interference from any RFID of a person sitting in the passenger seat.

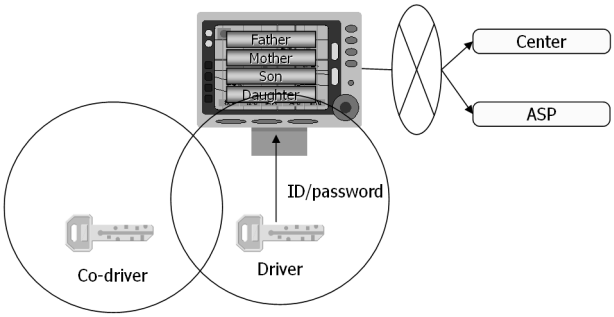

Fig. 14. Selecting from menu with an RFID device

7) Selecting the PKI function: Figure 15 shows an outline of the method to select the PKI function by touch with a finger. This method is a secure method for two or more people. The key to two or more people per secure device is registered, and it is selected from the menu. As a result, the driver's digital certificate is transmitted to the center and the user authentication is done. When renting an automobile, it is also possible to use a contactless smart card as a subcard of this secure device.

[3]Two kinds of authentication systems are needed for PKI and biometrics.

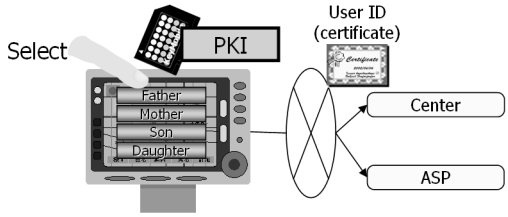

Fig. 15. Selecting the PKI function by touch

8) Select the PKI function with an RFID device: Figure 16 shows the selection of the PKI function with an RFID device. This is more convenient for the user than using a finger to touch the display. However, again it is necessary to prevent interference from any RFID of a person in the passenger seat.

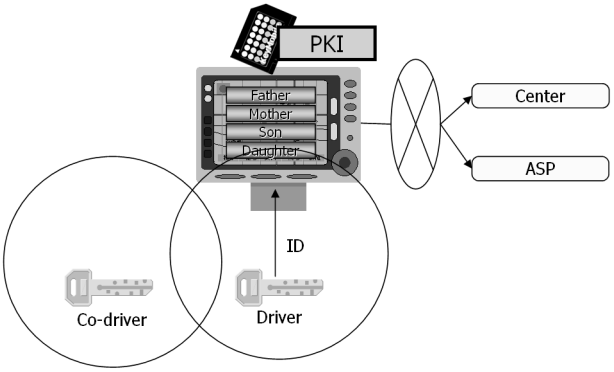

Fig. 16. Selecting a PKI function with an RFID device

9) Comparison of methods: Table II compares the methods described above with respect to adaptability to the user situation, convenience, and technical feasibility.

V. APPLICATION

In this section, we consider application of the proposed system in cooperation with other systems. Because the proposed system enables individual authentication, rather than authentication for the car (e.g., the car navigation system), the current driver can be specifically identified and provided services tailored for his preferences.

Here, we consider an example of application in cooperation with a security & safety (S&S) service. Figure 17 shows how such a coordinated system would operate.

In the S&S service, the data communication module (DCM) number is related to the serial number of the car, and the DCM reports the DCM number to the S&S service provider in the event of an accident. The S&S service provider reports the serial number of the car (and the date) as a key, and sends an inquiry to the center. The proposed system can provide the driver's information to the S&S service provider because it has authenticated the user who is currently driving a car. Thus, the car involved in the accident will be specified. Other information regarding a driver involved in an accident (name, age, sex, blood type, etc.) can also be provided through cooperation with the proposal system. Thus, customized S&S service for each driver becomes possible.

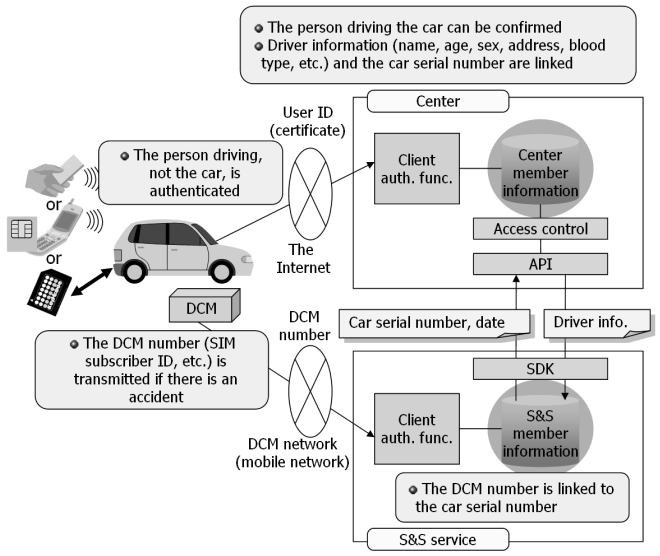

Fig. 17. Example

VI. CONCLUSION

In this work, we have considered how the telecommunication environment that surrounds a vehicle has changed, and will continue to change, and have determined the requirements for an authentication infrastructure. The telematics authentication infrastructure can meet these requirements. We divided the user authentication into that (1) between a person and a terminal, (2) between a terminal and a center, and (3) between the terminal and an ASP, and proposed methods appropriate for No.(1) and No.(2) type of authentication. These methods enable the center and the ASP to authenticate the individual who is driving a particular car. Therefore, it enables the provision of customized services according to the driver and the current situation.

We plan to soon implement the proposed methods, and to then evaluate them with regard to performance and user convenience.

Display concerning trademark etc.

– WiMAX, WiMAX Forum is a registered trademark of WiMAX Forum
– Global Platform^{TM} is a registered trademark of Global Platform Inc.
– Bluetooth is a trademark and a registered trademark of Bluetooth-SIG Inc. in the U.S.A.
– KeyMobile is a registered trademark of Hitachi Ltd.
– MMC (Multi Media Card) is a registered trademark of Infineon Technologies.
– miniSD^{TM}, microSD^{TM} is a trademark of the SD Card Association.
– In addition, any company name or product name that has been used is the trademark or registered trademark of the respective company.

REFERENCES

[1] K. Umezawa, A. Takahashi, H. Uchiyama, H. Sakazaki, M. Oikawa, S. Susaki, S. Hirasawa: "Development of certificate verification system for mobile services," IEICE Technical Report (IT), pp. 49-54 (2005)

TABLE II
COMPARISON OF METHODS

Method between terminal and center	Storage of confidential info.	Details of method	User device	Evaluation	Remarks
ID/ Password method	Terminal	Two or more ID/Passwords are registered in the navigation terminal beforehand. ID/Password is transmitted to the center by selecting them.	Select from menu with finger	Fair	Not applicable in a car-sharing system.
			RFID (Smart Key, etc.)	Good	Necessary to adjust the signal range to distinguish the signal from that of any RFID of a passenger.
			Contactless smart card	Fair	Taking out of a purse or a bag is troublesome.
			Cellular phone (NFC)	Good	
			Cellular phone (Bluetooth)	Good	
			Biometrics device (finger vein)	Good	
	User device	ID registered in the user device is transmitted to the center by way of the terminal.	Input by user	Poor	Troublesome to input the password every time.
			RFID (Smart Key, etc.)	Good	Necessary to adjust the signal range to distinguish the signal from that of any RFID of a passenger.
			Contactless smart card	Fair	Taking out of a purse or a bag is troublesome.
			Cellular phone (NFC)	Good	
			Cellular phone (Bluetooth)	Good	
			Biometrics device (finger vein)	Good	
PKI method	Terminal	The private key, the certificate, and the PKI operation function are mounted on the terminal.	select from menu with finger	Fair	The private key cannot be taken out, so cannot be applied to a rent-a-car system, etc.
			RFID (Smart Key, etc.)	Fair	Ditto
			Contactless smart card	Fair	Ditto
			Cellular phone (NFC)	Fair	Ditto
			Cellular phone (Bluetooth)	Fair	Ditto
			Biometrics device (finger vein)	Fair	Ditto
		The private key, the certificate, and the PKI operation function installed in the secure device set in the terminal are used.	Select from menu with finger	Good	
			RFID (Smart Key, etc.)	Good	
			Contactless smart card	Fair	Taking out of a purse or a bag is troublesome.
			Cellular phone (NFC)	Good	
			Cellular phone (Bluetooth)	Good	
			Biometrics device (finger vein)	Good	
	User device	The private key, the certificate, and the PKI operation function installed in the user device are used.	Select from menu with finger	Poor	Impossible
			RFID (Smart Key, etc.)	Fair	few RFIDs correspond to PKI
			Contactless smart card	Fair	Taking out of a purse or a bag is troublesome.
			Cellular phone (NFC)	Fair	Few cellular phones correspond to PKI
			Cellular phone (Bluetooth)	Fair	Few cellular phones correspond to PKI
			Biometrics device (finger vein)	Good	Ditto

[2] K. Umezawa, A. Takahashi, H. Uchiyama, H. Sakazaki, M. Oikawa, S. Susaki, S. Hirasawa: "Development and evaluation of certificate verification system in mobile environment," Computer Security Symposium 2005, p.p.121–126, (2005)

[3] K. Umezawa, M. Oikawa, S. Susaki, S. Hirasawa: "Evaluation of certificate verification method in mobile environment," Society of Information Theory and its Application (SITA) Symposium (2005)

[4] K. Umezawa, S. Susaki, S. Tezuka and S. Hirasawa, "Development and Evaluation of a Certificate Validation System in Mobile Environments," IEEJ Transactions of Electrical & Electronic Engineering (TEEE), 2007/1.

[5] K. Umezawa, M. Oikawa, S. Susaki, S. Tezuka: "Evaluation of certificate verification methods in mobile environment," IEICE Vol. J90-D No. 2 pp. 384-398, (2007)

[6] K. Umezawa, M. Oikawa, S. Susaki, S. Tezuka, S. Hirasawa: "Development of a Certificate Validation System for a Mobile Network," Information Processing Society of Japan (IPSJ) Journal, Vol.48 No.2, pp. 625-634 (2007)