An Authentication System using Smart Phones as Secure Storage

Katsuyuki UMEZAWA
Yokohama Laboratory
Hitachi, Ltd.
Kanagawa, Japan
katsuyuki.umezawa.ue@hitachi.com

Satoru TEZUKA
School of Computer Science
Tokyo University of Technology
Tokyo, Japan
tezuka@cs.teu.ac.jp

Shigeichi HIRASAWA
Information Technology and Business
Cyber University
Tokyo, Japan
shigeichi_hirasawa@cyber-u.ac.jp

***Abstract*—The smart phone penetration rate has increased recently. There are also many commercial terminals for receiving network services. When a service is received by a smart phone or PC, user authentication is very important for ensuring secure and safe use. Currently, authentication is required each time a user changes the terminal on which a service is received. We propose a system that uses a smart phone as a storage device for authentication information, such as ID, password, and cookie information. With this system, the smart phone and various terminals cooperate through short distance wireless telecommunications technologies such as Bluetooth. We evaluate performance of our proposed system. As a result, the user can input authentication information to and receive a service on a terminal by simply swiping the smart phone over the terminal.**

***Index Terms*—Mobile Terminal, Smart Phone, Secure Device, Authentication, ID Federation, Bluetooth**

I. Introduction

The smart phone penetration rate has increased recently, e.g., some people own two or more smart phones. There are also many commercial terminals for receiving network services. When a service is received by a smart phone or PC, user authentication is very important for ensuring secure and safe use. It would be convenient for the smart phone to be able to store the user's ID and password and be able to input that information into Web forms automatically by simply being swiped over a PC. Moreover, user convenience would improve greatly if the smart phone replaced, for example, hardware tokens for authentication, smart cards for merchant settlement, and car keys in a car sharing system.

To achieve this convenience and security, we propose an authentication system that uses the smart phone as storage for authentication information. We developed and evaluated a system that simplifies authentication at the server side when a user switches from an old terminal to a new terminal by storing the successive ID/password or cookie as authentication information.

A federation technology for the terminal has been proposed [8][9][10]. In these conventional studies, the target protocol was the ID Web Service Framework (ID-WSF)[8]; the purpose was joint ownership of a bookmark over a server[9] and federation of the multimedia content using the Digital Living Network Alliance (DLNA)[10]. These were not federation technologies for authentication by the server through use of a cookie or ID/Password.

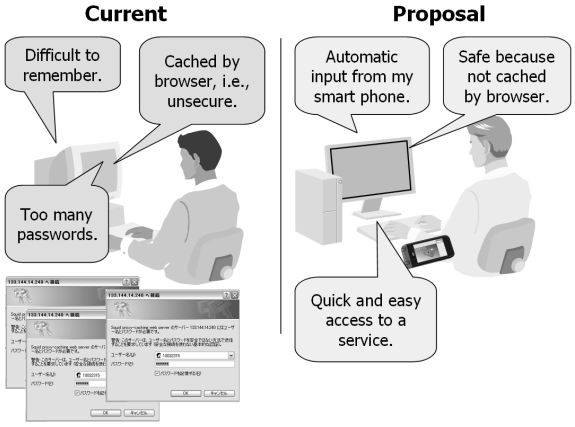

Fig. 1. Use case: accessing Web service

In Section 2, we describe the current problem situation and the advantages of our proposed system for authentication when Web services are used. In Section 3, we discuss related work, such as single sign-on, authentication using cookie information, and a handover technique that uses near field communication. In Section 4, we describe the proposed system. Specifically, we detail how the system coordinates information such as ID/password or cookie information inside and outside of a user's office. In Section 5, we evaluate our proposed system. Section 6 concludes this paper.

II. Current Problem and Advantage of Proposal

The problem with inputting IDs/passwords when Web services are accessed in illustrated in Fig. 1. Currently, an ID is individually assigned to various services as shown in Fig. 1, and it is necessary to also input the password for each ID. Moreover, a password change is often required in the short term according to the service policy. Remembering many IDs and passwords can be quite difficult. This information can be cached by Web browsers, but this is unsecure, e.g., the cached password might be used without permission if the terminal is shared. Convenience and safety can be improved if IDs/passwords are cached on a smart phone that an individual owns, and the smart phone can be swiped over a terminal to transfer the information.

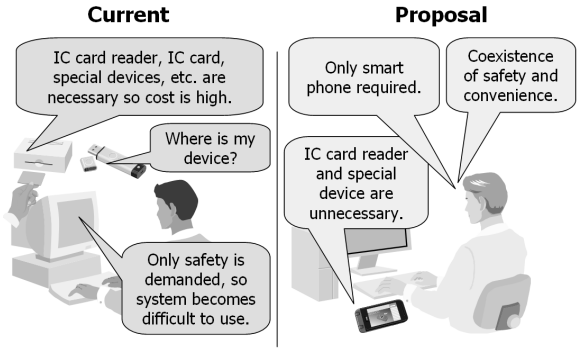

Fig. 2. Use case: accessing intranet

Figure 2 shows an example of a system that prioritizes safety over convenience of ID/password entry. A smart card reader and other special devices become unnecessary if the smart phone is used as an authentication token (storage for authentication key) as shown in Fig. 2.

The internal data would not be leaked because it is protected by the personal identification number (PIN) even if the phone was stolen. In addition, safety is increased by use of a remote lock and wipe function that mobile operators offer.

III. Related Work

A. Single Sign-On (SSO)

The problem of having to input IDs/passwords many times was explained in Fig. 1. This problem can be solved by using single sign-on (SSO), as long as the same terminal is used. Our proposed system aims to exchange authentication information between terminals, so different terminals can be used.

B. Authentication by Cookies

Cookies manage the state of Web browsers that use the HTTP(Hypertext Transfer Protocol) protocol. For instance, the visit history, log-in information, etc. for a Web site are preserved by the Web browser, and the log-in process can be skipped by transmitting the preserved cookie information when the same Web site is visited again. Cookies are defined in RFC2109 [1] and RFC2965 [2].

C. Near Field Communication (NFC) Handover

Near field communication (NFC), a handover technology, is defined by the NFC Forum. NFC handover is the connecting technologies between terminals; establishment of the relation between a terminal and another terminal (pairing) is done only with NFC (ISO 14443 Type A, Type B, FeliCa etc.). After pairing, terminals send and receive data by using higher-speed communication technology such as Bluetooth or Wi-Fi [3].

D. Remote Access Technology with Smart Phone

We have proposed a system that considers the smart phone terminal to be a secure device [4][5][6]. However, the smart phone terminal and PC terminal combination was fixed in this system. For instance, when we use a shared PC terminal, it was necessary to change the combination of a smart phone and a shared PC terminal.

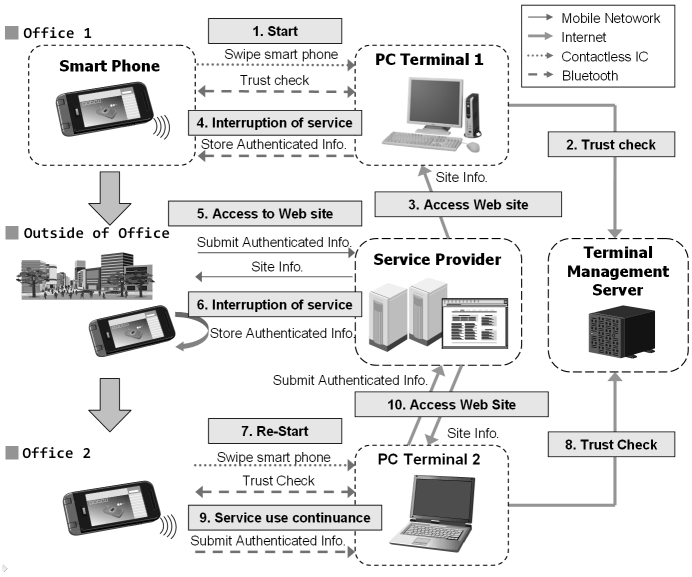

Fig. 3. Outline of proposed system

E. Other federation technology

ID-WSF[7], which is a specification enabling a user to log in to two or more sites with one terminal, is provided for in the Liberty alliance. Fujii et al.[8] are enhancing ID-WSF so that two or more terminals may federate. The authentication information, which is called an assertion, is transferred between terminals.

Miyakawa et al. have proposed cooperation across devices as an upgrade of the IPTV service[9]. The technology proposed here shares bookmark and resumes information. This information is shared with a mobile terminal and the IPTV terminal through the server, not through local communication between terminals.

In addition, Nagai has proposed federation technology for cellular phone networks[10]. This enhances the DLNA[11], which controls multimedia contents, so that it can handle mobile terminals. Though it is technology for coordinating the multimedia contents, it is not federation technology for authentication by the server.

IV. Proposal

We describe the proposed system in this chapter.

A. Outline of Proposal System

An outline of our proposed system is shown in Fig. 3 and described below.

- The user transmits an ID/password from the smart phone to a form on a Web browser automatically by swiping the smart phone over PC terminal 1 and then is connected to the service provider server automatically. When the Web authentication succeeds, the service provider server issues a cookie for the information that has been authenticated. The cookie information is stored in the smart phone (Office 1 in Fig. 3).

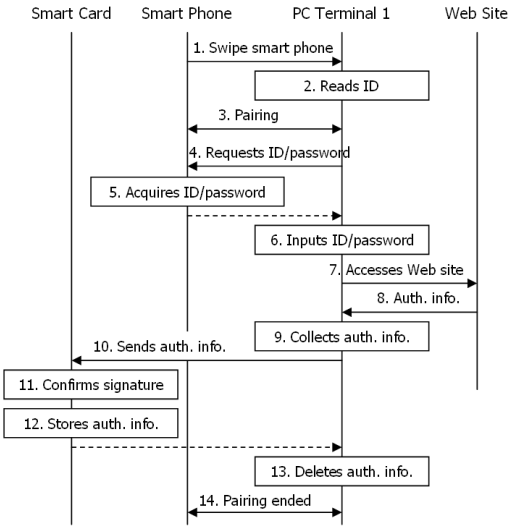

Fig. 4. Sequence when using PC terminal 1

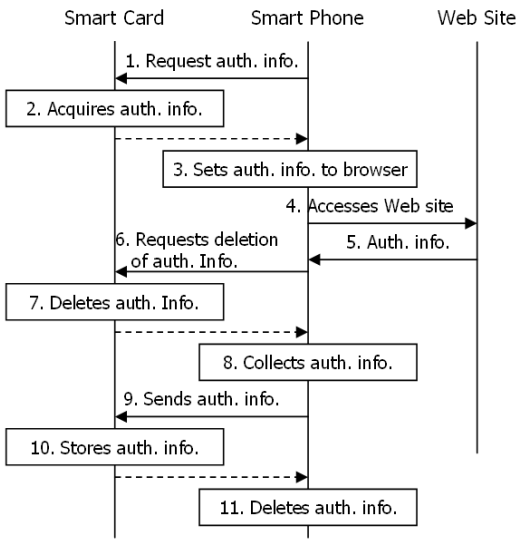

Fig. 5. Sequence when using smart phone

- The cookie information is set in the smart phone's browser when a service is received by the smart phone. The smart phone's browser connects with the service server, and the service is then received (Outside of Office in Fig. 3).
- Finally, if the user moves to another office and tries to access the service on another terminal (PC terminal 2), cookie information stored in the smart phone is transmitted to that terminal by simply swiping the smart phone over the terminal. The cookie is set in the browser on PC terminal 2, the browser connects with the service provider server, and service is received (Office 2 in Fig. 3).

Transmitting password and cookie information to a terminal that cannot be confirmed as safe is unsecure. It is necessary to secure the safety of a PC terminal through the reliability confirmation function in Fig. 3 (Please refer to section IV-D for the details.).

B. Sequence of Proposed Method

In this section, we detail the sequences of the proposed method in the three use cases shown in the previous section.

- In the office (Office 1), the user receives a service on PC terminal 1 by swiping a smart phone over that terminal.
- Outside the office, the user receives a service on his or her smart phone while moving.
- In another office (Office 2), the user receives a service on PC terminal 2 by swiping the smart phone over that terminal.

1) Sequence when using PC terminal 1: The smart phone is swiped over PC terminal 1, service is received on that terminal, and the authentication information is transmitted to the smart phone. Figure 4 shows this sequence.

1) The smart phone is swiped over PC terminal 1.
2) PC terminal 1 reads the FeliCa ID.
3) Bluetooth pairing occurs between PC terminal 1 and the smart phone[1].
4) PC terminal 1 requests ID/password information to log-in to a Web site from the smart phone.
5) The smart phone retrieves the ID/password information stored within itself and sends it to PC terminal 1.
6) PC terminal 1 executes a browser or searches a browser under execution and inputs the ID/password information.
7) The user accesses the service provider site on PC terminal 1.
8) Authenticated information (a cookie) is issued from the site, and the service is received.
9) PC terminal 1 collects the authentication information that its browser manages.
10) PC terminal 1 sends the collected authentication information to the smart card in the smart phone.
11) The smart card confirms the signature for the command.
12) The smart card writes the received authentication information to itself.
13) PC terminal 1 deletes the authentication information that its browser manages.
14) The pairing between PC terminal 1 and the smart phone is ended.

2) Sequence when using smart phone: Figure 5 shows the process flow for receiving a service continuously by using the authentication information stored on the smart card in the smart phone. The flow in this figure is explained next.

1) The smart phone requests the authentication information from the smart card.
2) The authentication information stored in the card is retrieved and sent to the smart phone.
3) The smart phone stores the received authentication information in its browser.

[1]A pass phrase is shared through the pairing, and the subsequent command will be encrypted

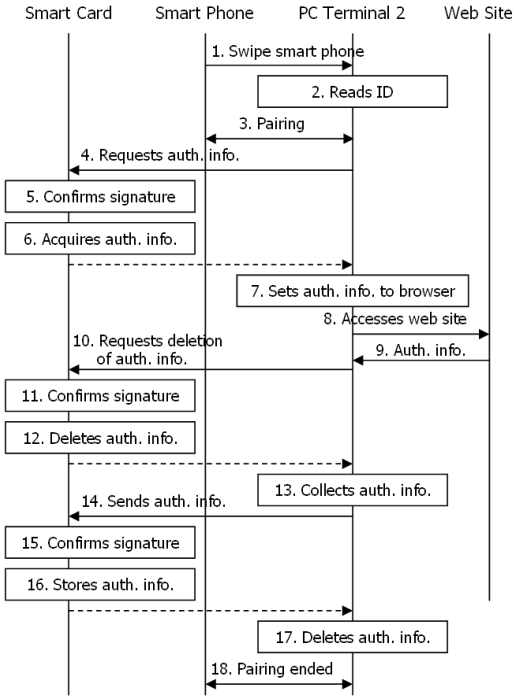

Fig. 6. Sequence when using PC terminal 2

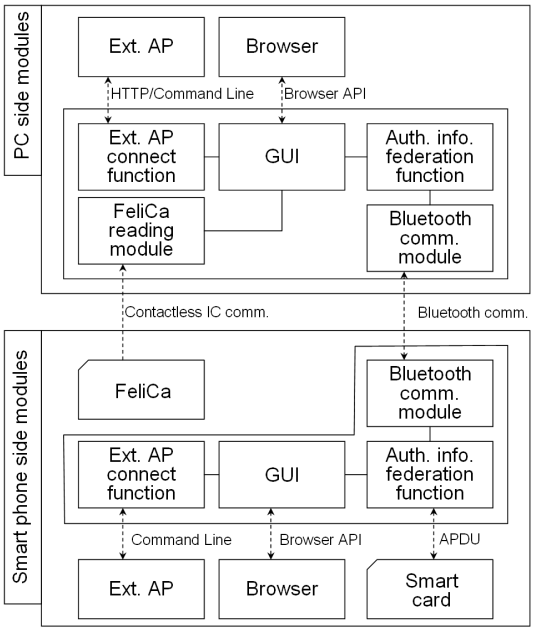

Fig. 7. Module structure of proposed system

4) The user accesses the service provider site from the smart phone.
5) The authentication information is issued from the site, and the service is received.
6) The smart phone requests deletion of the authentication information from the smart card.
7) The smart card deletes the stored authentication information.
8) The smart phone collects the authentication information that its browser manages.
9) The smart phone sends the acquired authentication information to the smart card.
10) The smart card writes the authentication information to itself.
11) The smart phone deletes the authentication information that its browser manages.

3) Sequence when using PC terminal 2: The smart phone is swiped over PC terminal 2, and the authentication information succeeded from PC terminal 1 is transmitted to PC terminal 2. As a result , service is received continuously with PC terminal 2. This flow is shown in Fig. 6 and is explained next. Note that Items 13 to 18 are the same as Items 9 to 14 in Fig. 4 so they are not explained here.

1) The smart phone is swiped over PC terminal 2.
2) PC terminal 2 reads the FeliCa ID.
3) Bluetooth pairing occurs between PC terminal 2 and the smart phone.
4) PC terminal 2 requests authenticated information (a cookie) from the smart card in the smart phone.
5) The smart card confirms the signature for the command.
6) The smart phone acquires the authentication information stored on the smart card and sends that information to PC terminal 2.
7) PC terminal 2 stores the received authentication information in its browser.
8) The user accesses the service provider site through PC terminal 2.
9) The authentication information is issued from the site, and the service is received.
10) PC terminal 2 requests the deletion of the authentication information from the smart card in the smart phone.
11) The smart card confirms the signature for the command.
12) The smart card deletes the authentication information stored on itself.

C. Module structure of proposed system

In this section, we describe the module structure of the proposed system. Figure 7 shows the function modules on the PC terminal side and the function modules on the smart phone side.

The PC side is composed of the following functional modules (Fig. 7).

- **GUI:** sets parameters in communication tools and displays the log.
- **Authentication information federation function:** sends and receives authentication information, such as ID/password and cookie, to the smart phone through Bluetooth communication.
- **External AP connect function:** transmits commands from external applications on the PC terminal for the transmission, deletion, etc. of the authentication information to the authentication information federation function module.

- **Bluetooth communication module:** executes Bluetooth pairing of the smart phone by using the FeliCa ID, read by the FeliCa reading module, and sends and receives the data to and on the smart phone.
- **External AP:** external application related to the service.
- **Web browser:** browser for Web service.
- **FeliCa reading module:** waits for FeliCa to be held up and the FeliCa ID.

The smart phone side shown in Fig. 7 is composed of the following functional modules.

- **GUI:** sets parameters in communication tools and displays the log.
- **Authentication information federation function:** sends and receives the authentication information such as ID/password and cookie to the PC terminal through Bluetooth communication.
- **External AP connect function:** transmits commands from external applications on the smart phone for the transmission, deletion, etc. of the authentication information to the authentication information federation function module.
- **Bluetooth communication module:** executes Bluetooth pairing of the PC terminal by using the FeliCa ID, and sends and receives the data to and on the PC terminal.
- **External AP:** external application related to the service.
- **Web browser:** browser for Web service.
- **FeliCa:** contactless integrated circuit chip.
- **Smart card:** integrated circuit chip that stores authentication information etc.

D. Confirming reliability of terminal

In this work, we supposed a PC terminal to be safe and proposed a cooperative method for sharing authentication information. However, many terminals are not safe, e.g., jointly owned terminals and public terminals. For such cases, the following method is being considered[2].

- The terminal uploads inventory information to the server regularly.
- The terminal acquires evidence (trusted certification data) from the server that no malicious applications are installed on itself.
- The terminal adds trusted certification data to a command to transmit to IC chips and checks this data on the chips.

V. Evaluation

We evaluated the performance of our system by measuring the time taken for processing in the ID/password federation technique and processing in the cookie federation technique.

A. Measurement conditions

The specifications of the terminals for which performance was measured are shown in Tables I and II. FeliCa was used for contactless IC communication between terminals. Bluetooth

[2]The details of confirming the reliability of a terminal will be presented in a later paper.

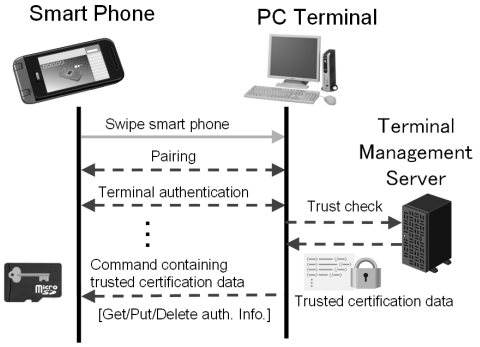

Fig. 8. Confirming reliability of terminal

TABLE I
SPECS OF PC USED FOR MEASUREMENT

OS	Windows XP SP3
CPU	Intel Core2 Duo T8100 (2.10 GHz)
Memory size	3 GB
Browser	Internet Explorer 8

Ver. 2.1 was used for the Bluetooth communication after the handover. In addition, we used three kinds of networks between the PC and server: a cable LAN network, ADSL communication network, and 3G data communication named CDMA 1X WIN.

B. Measured items

We measured the time taken for the following sequences.

- Processing in federation of smart phone and PC terminal1
  (1-1) Log-in by ID/password federation (steps 1 to 8 in Fig. 4)
  (1-2) Transfer of authenticated information from PC terminal 1 to smart card (steps 9 to 14 in Fig. 4)
- Processing on smart phone
  (2-1) Log-in with smart phone unit(steps 1 to 5 in Fig. 5)
  (2-2) Deletion of authenticated information in smart card in smart phone (steps 6 to 7 in Fig. 5)
  (2-3) Transfer of authenticated information in smart phone to smart card (steps 8 to 11 in Fig. 5)
- Processing in federation of smart phone and PC terminal2

TABLE II
SPECS OF SMART PHONE USED FOR MEASUREMENT

OS	Windows Mobile 6.5 Professional Edition
CPU	Qualcomm QSD8650 1 GHz
Memory size	512 MB (ROM)/384 MB (RAM)
Browser	Internet Explorer Mobile

TABLE III
NETWORK SPECS USED FOR MEASUREMENT

Cable LAN	Gigabit Ethernet
ADSL	8 Mbps (downstream)1 Mbps (upstream)
3G	2.4 Mbps (downstream)114 Kbps (upstream)

TABLE IV
MEASUREMENT RESULTS

No.	Process	Time (Sec)
(1-1)	Log-in by ID/password federation	1.71 (LAN), 1.74 (ADSL), 2.52 (3G)
(1-2)	Transfer of authenticated information from PC terminal 1 to smart card	4.60
(2-1)	Log-in with smart phone	10.48 (3G)
(2-2)	Deletion of authenticated information in smart card in smart phone	2.03
(2-3)	Transfer of authenticated information in smart phone to smart card	3.03
(3-1)	Log in by authenticated information federation	5.04 (LAN), 5.34 (ADSL), 9.37 (3G)
(3-2)	Deletion of authenticated information in smart card from PC terminal 2	3.87

(3-1) Log-in by authenticated information federation (steps 1 to 9 in Fig. 6)
(3-2) Deletion of authenticated information in smart card from PC terminal 2 (steps 10 to 12 in Fig. 6)
(3-3) Transfer of authenticated information from PC terminal 2 to smart card (steps 13 to 18 in Fig. 6. However, we did not measure this because it is the same as (1-2).)

C. Measurement Results

In this section, we describe the details and results of measuring the time taken for processing of each measurement item. We measured each item 12 times, excluded the minimum and maximum results, and calculated the mean value for each item from the remaining 10 measurements. The results are shown in Table IV. To summarize, using the cookie method, users can log in to the system within ten seconds, or within three seconds using ID and password[3][4].

VI. CONCLUSION

We propose a both convenient and safe authentication system that uses a user's smart phone as a "key" when the user needs to be authenticated. Our system stores authentication information, such as IDs/passwords and cookie information, in the smart phone and uses contactless IC communication and short distance wireless telecommunications such as Bluetooth. The user can be authenticated by simply swiping the smart phone over a PC terminal. We developed a prototype system and evaluated its performance. To summarize, using the cookie method, users can log in to the system within ten seconds, or within three seconds using ID and password. With our proposed system, the user can be automatically authenticated by simply swiping the smart phone over a terminal, and he or she can then receive services on that terminal.

In the future, we will enhance our system to work with short distance wireless telecommunications other than Bluetooth, such as Wi-Fi and ZigBee. We will also extend it to a variety of smart phone terminals.

[3]As steps (1-2), (2-2), (2-3), and (3-2) can be processed after authentication, they will not affect usability.

[4]Most of the 10.48 seconds taken for Item (2-1) is for IC access.

ACKNOWLEDGMENTS

This study is a part of the "Research and development of terminal platform technology" project sponsored by the National Institute of Information and Communications Technology (NICT).

TRADEMARK INFORMATION

- Bluetooth is a registered trademark of Bluetooth-SIG Inc.
- Wi-Fi is a registered trademark of Wi-Fi Alliance
- FeliCa is a registered trademark of the Sony Corporation.
- Windows, Windows Mobile, and Internet Explorer are registered trademarks of the Microsoft Corporation in the U.S.A and other countries.
- Intel and Intel Core$^{\mathrm{TM}}$ are registered trademarks of the Intel Corporation and their subsidiary companies in the U.S.A and other countries.
- Qualcomm is a registered trademark of the QUALCOMM Incorporated.
- ZigBee is a registered trademark of the ZigBee Alliance.
- CDMA 1X WIN is a registered trademark of the KDDI Corporation.

REFERENCES

[1] D. Kristol and L. Montulli, RFC2109: HTTP State Management Mechanism, IETF(Internet Engineering Task Force), Feb. 1997.

[2] IETF RFC2965 HTTP State Management Mechanism
D. Kristol and L. Montulli, RFC2965: HTTP State Management Mechanism, IETF(Internet Engineering Task Force), Oct. 2000.

[3] Connection Handover Technical Specification, NFC(Near Field Communication) Forum, Nov. 2008

[4] Katsuyuki Umezawa and Seiichi Susaki, "Development of a remote access system with smart phone," Proceeding of the 31st Symposium on Information Theory and Its Applications, pp. 971–974, Oct. 2008.

[5] Katsuyuki Umezawa, Takatoshi Kato and Satoru Tezuka, "Development of FMC Authentication Technique with Mobile Terminal," IEICE(The Institute of Electronics, Information and. Communication Engineers) Technical Report (ISEC2009-36, SITE2009-28, ICSS2009-50), pp. 203–208, Jul. 2009.

[6] Katsuyuki Umezawa, Takatoshi Kato and Satoru Tezuka, "Development and Evaluation of a Remote Access System with Smart Phone," Proceeding of 8th Forum on Information Technology (FIT2009), Volume 4, pp. 67–73, Sep. 2009.

[7] Liberty Alliance, "Liberty Alliance ID-WSF 1.1 Spesifications," http://www.projectliberty.org/resource_center/specifications/liberty _alliance_id_wsf_1_1_1_specifications.

[8] Arisa Fujii, Kiyohiko Ishikawa, Toshiharu Morizumi, Yumi Kikuchi, Tomokazu Yamada, Masahito Kawamori, Katsuhiko Kawazoe, "Seamless viewing service for multi-device users by accession of authentication information," The Institute of Image Information and Television Engineers Technical Report, 32(37), pp. 21–26, 2008-09-25.

[9] Miyakawa Kazu, Hibino Sou, Horiguchi Kyoutarou, Seshimo Hitoshi, Fukada Satoshi, Takahashi Tatsunori, Yamada Tomokazu, NTT Technical Journal, pp.12–17, Oct. 2009 (In Japanese)

[10] Takeshi Nagai, "Network Connectivity Technologies for Mobile Devices," Toshiba Review, Vol.64, No.12, pp.37–40, 2009.

[11] DLNA Networked Device Interoperability Guidelines v1.5.