APPLICATION TO A SHARED TERMINAL OF A ROAMING USER PROFILE SET UP THROUGH LDAP-SMART CARD AUTHENTICATION COOPERATION

Kazuto Kuzuu, Yasushi Hirano, Kenji Mase and Toyohide Watanabe
Information Technology Center, Nagoya University, Furo-cyo, Chikusa-ku, Nagoya-shi, Aichi-ken, Japan

Keywords: Smart card, LDAP, authentication, user profile, shared terminal.

Abstract: In this paper, we propose the way to set a roaming user profile without using Windows domain composition when building a shared terminal system for smart card users. This proposal aims at using a LDAP server as a user information data base, and enabling each terminal user to set his own work environment. In order to achieve this purpose, we related the user profile with the user ID extracted from smart card, and stored that profile on shared data storage. Furthermore, we built a shared file system besides the above data storage, and assigned the user work environment to that file system. Finally, applying the above system to the actual terminal on network, we confirmed that the target shared terminal environment was realized.

1 INTRODUCTION

A shared terminal is often set up so that a guest user cannot log off freely since it is placed in a public facility and used by unspecified persons. In such situations, even operations by a mouse and a keyboard are severely restricted on the terminal.

On the other hand, shared terminal users are increasing by means of the spread of smart cards and the improvement of security technology. This tendency is remarkable especially in a company. This increase might be due to the fact that the smart card authentication can provide improvement for security as well as convenience for the usage of PC. From this point, it can be said that introducing smart card is indispensable to a shared terminal.

In order to explore how to use a shared terminal in the university, we have so far developed the application and the middleware for smart card logon by ourselves. Then, we made the Java Card™ application which works by Java Card™ technology (Chen, 2004) and makes use of PKI frame work. And using this application, we implemented the middleware for smart card authentication into Windows system (Kuzuu et al., 2006).

Furthermore, we introduced new concept for user profile roaming into smart card logon system. In this system, we can build each user environment on a shared terminal during logon process without depending on Windows domain system. User account management for a shared terminal is usually performed based on the user account information on a domain control server. However, this brings a system administrator much burden, since he has to introduce a domain server and manage directory information doubly. In order to avoid this problem, we have proposed the system which can provide individual environment, without introducing a domain control server (Kuzuu et al., 2007).

In this paper, improving further the above-mentioned system, we propose the system which can hold the individual data related to each user profile on a share terminal without being based on domain composition.

2 CONSTRUCTION OF THE SYSTEM

2.1 Shared Terminal System Configuration

This shared terminal system has the feature that a user can rebuild his work environment during logon process without constituting Windows domain. First, we show the basic configuration of this system. This system is composed of three components connected to network. They are LDAP server for user

Kuzuu K., Hirano Y., Mase K. and Watanabe T. (2008).
APPLICATION TO A SHARED TERMINAL OF A ROAMING USER PROFILE SET UP THROUGH LDAP-SMART CARD AUTHENTICATION COOPERATION.
In *Proceedings of the International Conference on Security and Cryptography*, pages 29-34
DOI: 10.5220/0001930100290034

information, data storage for user profile and shared file system for user data. Figure 1 shows the present system configuration.

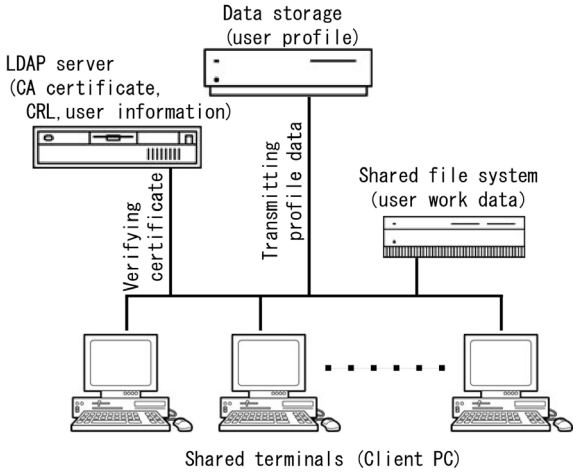

Figure 1: Shared terminal system configuration not using a Windows domain.

2.2 Construction of Smart Card Authentication

Logon authentication by smart card, which is called smart card logon, plays a significant role about the security in a shared terminal, and is beginning to be implemented into many PCs recently. In this research, using Java Card™ technology, we installed Java Card™ application, by which digital certificates can be stored, into a smart card, and then implemented the logon authentication middle ware, which communicates with a smart card and LDAP server, into Windows system. Through the above-mentioned application and middleware, we added the function of smart card logon, which cooperated with PKI, into a shared terminal (Kuzuu et al., 2006).

Here, in the development of this authentication program, we made use of the extended API of GINA, Graphical Identification and Authentication, which is normally implemented into Windows XP and Windows 2000 systems. On the other hand, in order to embed PKI into the authentication system, we built a private CA by introducing NAREGI-CA (Okuno, 2004), and adopted a directory server, OpenLDAP 2.3 as a data base which can manage CA certificate and CRL, Certificate Revocation List.

2.3 Data Storage for Roaming User Profile

In Windows system, the user environment is provided through loading of the user profile data from the registry during logon process. Here, the user profile data is classified into a local user profile, a roaming user profile and a mandatory user profile. While a local user profile, unlike other profiles, is stored in a stand-alone machine, a roaming user profile and a mandatory user profile are stored in the server machine which manages a domain. Especially, a roaming user profile enables us to make our own environment since we can change a profile variable in person. In other words, the concept of such roaming user profile is required for making the individual environment in a shared terminal. However, a roaming user profile and a mandatory user profile can be set up only when the user account is registered on a Windows domain. The above-mentioned situation means that when the other directory server such as LDAP has already been introduced, the directory information must be managed doubly or it is necessary to synchronize two systems.

In order to avoid such a problem resulting from introducing a domain server newly and to satisfy the conditions of profile roaming, we proposed the system in which we can store individual user profile into data storage, logging on through smart card authentication accessing LDAP (Kuzuu et al., 2007).

In this system, while users log on a shared terminal as a guest user not belonging to a domain, the authentication is carried out through a smart card implementing PKI frame work. This means that the logon user of a shared terminal is not an anonymous user. On the other hand, the profile of logon user is saved at data storage by the file name related to the user ID stored in his smart card.

2.4 Assigning User Shell Folders to a Shared File System

As mentioned in 2.2, profile roaming in this system is realized by individual profile loaded from data storage to the terminal. During this process, the user can rebuild his work environment after the smart card authentication, even though he logs on as a guest user which cannot be distinguished on the shared terminal. However, in order to build an actual work environment, we have to make the user profile related to our own data, for example documents, desktop files, cookies, bookmark and temporary files etc. In such situation, the amount of user data is too large to store, and transmission to data storage wastes too much time.

2.4.1 Implementation of Samba File Server

In order to resolve the above problem, we made the user profile related to user shell folders on the shared file system during logon process. Here, we built the shared file system for saving user shell folders, implementing Samba file server on Linux machine. Through this setup, we can automatically connect to this file system after logon authentication. Figure 2 shows the sequential process from inserting a smart card to rebuilding a user work environment.

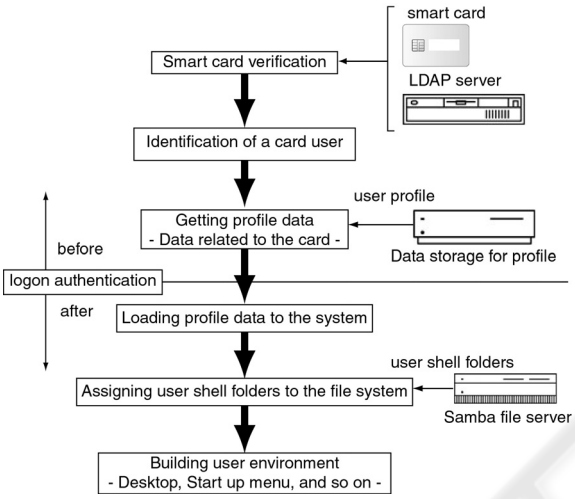

Figure 2: Logon process of shared terminal.

2.4.2 Network Drive Connection to a Shared File System

In Windows system, the user shell folders, for example Application data, Cookies, Desktop and My Documents, etc., usually exist in the user name folder within the Documents and Settings folder in a system drive, and the user data is saved in the folder corresponding to its purpose. In the present system, since a user account name is in agreement with the guest account name on a shared terminal, this data is saved in the same folder. This means that a smart card user, a shared terminal user, can access data which the other user leaves on that folder. In order to avoid sharing the folder which a different card user owns, we need to put the personal folder on the user directory registered individually on Samba shared file system. For this purpose, we make a shared terminal connect to the Samba file server during logon process, using the name of the user who possesses the smart card. Actually, we can connect to Samba file server as a smart card user, executing net use command as an external process after logon authentication of GINA process. In this system, the external process is described within the Create Process function of Win32 API, and then the specific drive is assigned for the connected samba file system. Furthermore, in order to access the personal folder on Samba, the terminal user has to be registered as a Samba user. However, it is not necessary that we input our own Samba password individually for connection, since this process is managed by GINA. This means that the user cannot access the Samba server from other computer than a shared terminal, even though the terminal user is registered as a Samba user. Considering this point, we can say that the security for the shared file system is assured.

2.4.3 Drive Assignment of the Shared File System

In this system, we need to make the user profile related to the user shell folders on the Samba file system so that the terminal user does not share the individual data. However, the system is not usually designed so as to refer to the user shell folders on the Samba file system when the user environment is built based on the user profile. Although we can specify the target of the My Document folder explicitly, an arrangement tool for other folders is not provided in Windows system.

In order to resolve this problem, we modified the user shell folder paths in the registry. In fact, we can specify the user folder path as parameters of registry key, \HKEY_USERS\S-*\Software\MicrosoftWindows\CurrentVersion\Explorer\UserShellFolder,using a registry editor. On the other hand, these parameters are stored in the data storage as a user profile data, NTUSER. DAT.

3 SYSTEM CONFIGURATION

In this section, we show configuration of software and hardware which are prepared for the present system.

3.1 Specification for Smart Card

The smart card used for this system is the type of dual interface and has 1MB memory, and Java Card™ VM is implemented in this card. The security API of this card enables basic crypto calculations, such as RSA, DES, T-DES, etc. The authentication application, by which PIN code, a user certificate and a private key can be stored into the smart card, was developed on Java Card™ VM using Java Card Technology. A user certificate is

subject to X.509 standard and encoded by DER format of ASN.1. A private key is 1024-bit RSA encryption key. Specifications of smart card and smart card reader are shown in Table 1 and 2.

Table 1: Specification of the smart card.

	Java Card™	
	contact	contactless
Standard	ISO/IEC7816	ISO/IEC 14442 Type B
Communications protocol	T = 0, 1	ISO/IEC14443-4
Transfer speed (max)	19.2 kbps	424.0 kbps
Memory	1MB (Flash memory)	
CPU	16bit	
Security	RSA, DES, T-DES implemented	

Table 2: Specification of the smart card reader.

	contact	contactless
Product name	GemPC TWIN	PD2992P
Standard	ISO/IEC7816	ISO/IEC 14442 Type B
Interface	USB 2.0	USB 1.1

3.2 Specification of Terminal and Server

In this implementation, we prepared ThinkCentre A52T(WindowsXP Professional SP4) and ThinkPad X41 Tablet(WindowsXP Professional SP4) as a virtual shared terminal, and DELL Power Edge 2850 3.8GHz Xeon & Cent OS5 as a data storage machine which can store user profile data. With respect to the latter machine, we implemented NAREGI-CA (Okuno, 2004) as CA, and OpenLDAP2.3 as a directory server. On the other hand, we also implemented the file system using Samba 3.0.10 on ThinkCentreA52T & Cent OS5.

3.3 Installation of Logon Middleware

The logon middleware developed in this study is installed into the virtual shared terminals. In this middleware, Windows CriptoAPI is employed as API associated with authentication and encryption. On the other hand, we made use of Win32 API for communication process to smart card and LDAP server. Development environment for this middleware is VC++ ver.6 and Platform SDK.

3.4 Issue of Certificate

A private CA was made in order to issue a certificate. CA server is NAREGI-CA shown in 3.2, and issue of CA certificate, a user certificate and CRL is performed through this CA. Furthermore, LDAP server is introduced as a repository in order to store each certificate and user directory information.

4 ACTUAL PROOF EXPERIMENTS

We carried out actual proof experiments for two smart card users who have both user certificate and private key in their card. The contents of verification are as follows.

- Verifying that each user can rebuild his user environment accessing the user's own profile during logon process.
- Verifying that the user shell folders are assigned to different directory on Samba file system according to each user.
- Verifying that the application environment set up for each user does not influence mutually.

3.1 Reconstruction of User Environments

First, we tried to do logon authentication using two smart cards A and B on the shared terminal in which the present system is implemented. As shown in Fig.3, we verified that the different desktop environments can be provided for each card user after logon. Next, we logged on from the terminals X and Y using smart card A. Although the terminals are different, we can confirm that the desktop environment is not changed as shown in Fig.4.

4.2 Assignment of User Shell Folders

In this system, we can automatically connect to the shared file system through Samba file server, and user folders on that file system are associated with user work environment. In this section, we verify that the user shell folders are assigned to Samba file system and each card user connects to their folders

as a Samba user related to their card. Figure 5 shows the user shell folders assigned to Samba users, myca000001 and myca000002. Each user account corresponds to user ID of the smart card.

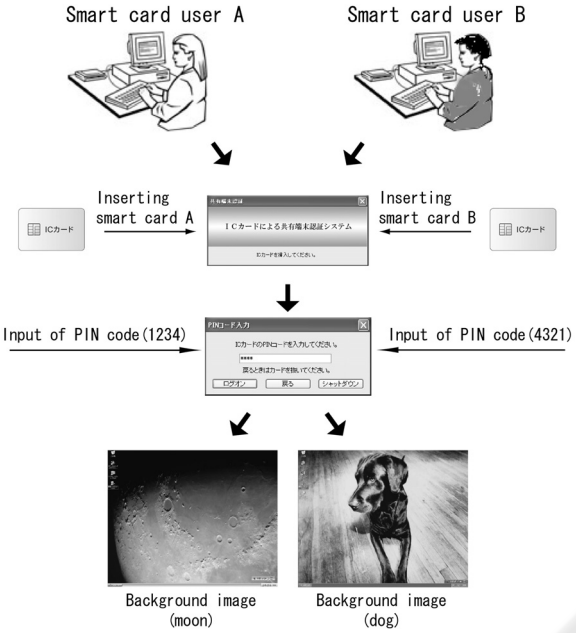

Figure 3: Desktop of different users on the same terminal.

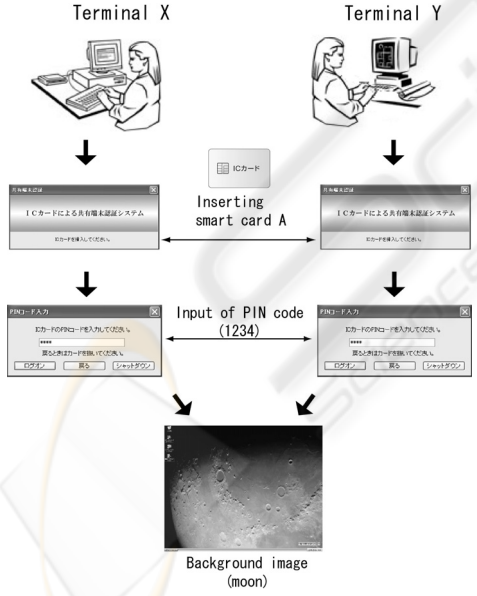

Figure 4: Desktop of a user on the different terminals.

4.3 Independency of Application Environment

Next, we investigated whether the parameter of some applications, such as initial values, options and format parameters, etc., can be independently specified for each user. Here, the applications used for this investigation are Internet Explorer, IE6, and LDAP browser.

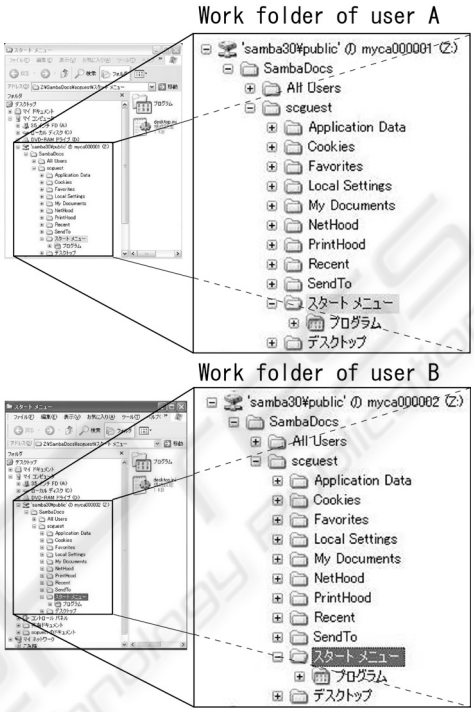

Figure 5: Work folder assignment on Samba.

After setting up these applications, we verified that the initial window, history data, book marks and default format, etc. are specified independently according to each user. Figure 6 shows comparison about initial windows and book marks of each card user. We could see that windows and menus are different in each user, and confirmed that the internet temporary file, cookies, viewing histories,

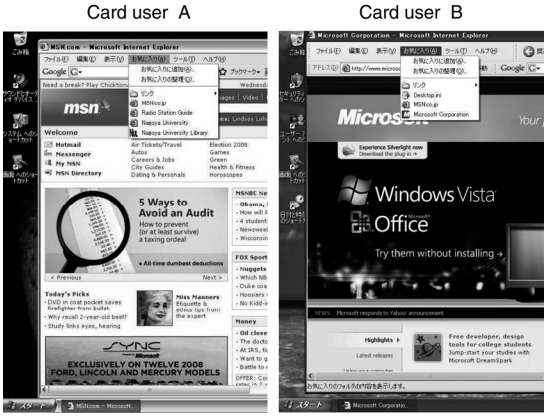

Figure 6: Comparison of user setting of IE6.

etc. are independently saved according to each user. Furthermore, as shown in Fig. 7, we also verified that a different input option for each user is maintained as setting menus of LDAP browser.

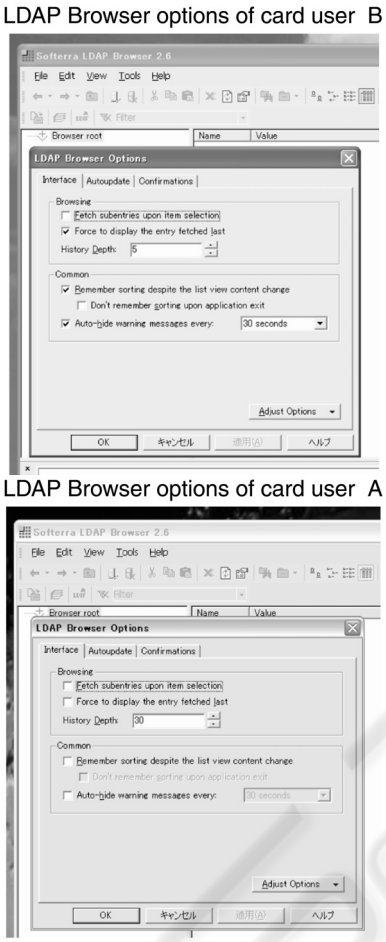

Figure 7: Comparison of user setting of LDAP browser.

5 CONCLUSIONS

We newly developed the system in which the individual user environments can be rebuilt on the shared terminal without participating in a domain, and we verified the validity of that system through the actual implementation on the virtual shared terminal. Especially, we enabled our system to rebuild the individual work environment for each user by putting the user shell folders on Samba file system different from a local machine. Then, we confirmed that this system can be regarded as advantageous solution from the points of both user management and economical efficiency. On the other hand, when considering how to use a shared terminal, we must assure the enough security and the functions of information management. These points might be the issues that we should consider in the future.

ACKNOWLEDGEMENTS

This research was carried out as a part of the Cyber Science Infrastructure, CSI, which is a project of National Institute of Informatics. We describe it here and express gratitude.

REFERENCES

Chen, Z., 2004. *Java Card™ Technology for Smart Cards*, Addison-Wesley.

Kuzuu, K., Hirano, Y., Mase, K., and Watanabe, T., 2006. Smart Card Logon for a Shared Terminal Computer based on PKI Authentication (Japanese), *Computer Security*, no.2006-CSEC-035, pp.45-50.

Kuzuu, K., Hirano, Y., Mase, K., and Watanabe, T., 2007. Implementation of IC Card Authentication System combined with Roaming User Profile not belonging to Domain into a Shared Terminal (Japanese), *Internet Conference 2007*, no.51, ISSN 1341-870X, pp.21-30.

Okuno, T., 2004. New open source CA development as Grid research platform, http://www.naregi.org/papers /data/ggf12 caops_pki.pdf, *Global Grid Forum*.