Application of Secure Information Sharing Platform Technology to E-government

Koji Kishi[†], *Seiji Takahashi, Kenji Murai, Takumi Kashiwagi, Yoshihiro Yoshida, Hirofumi Abe, and Takashi Ikeda*

Abstract

This article outlines our research and development of *secure information sharing platform technology* for the safe and reliable sharing of information in information technology systems and introduces a prototype system for an e-government platform.

1. Introduction

In recent years, information and communications technology (ICT) systems have increasingly come to be used in a variety of fields that affect our daily lives. Such systems require a mechanism for sharing information in a safe and reliable manner. In response to this need, we have been researching and developing *secure information sharing platform technology* to prevent information tampering and information leakage to unintended parties. Our secure information sharing platform technology consists of three components: scalable secure file sharing [1], information access control, and virtual smart card technologies (**Fig. 1**).

1.1 Scalable secure file sharing technology

This enables large electronic files to be transferred safely and reliably. In addition to data encryption using the Camellia cipher [2] and user/server mutual authentication by the public key infrastructure (PKI) scheme, it supports the issuing of delivery certificates in conjunction with a timestamping authority so that the user can confirm delivery of an electronic file to the intended party. Also included is a mechanism for resuming file transfer in the event of an interruption due to network faults or other problems.

† NTT Service Integration Laboratories
Musashino-shi, 180-8585 Japan

1.2 Information access control technology

This controls *who can perform what operations* on information on the server. Here, *who* can be indicated by specifying a particular individual or a certain relationship with the information owner. And *operations* refers to viewing, editing, or performing other actions on that information. For example, for information belonging to Mr. A, typical settings would let Mr. A's family view that information but allow only Mr. A himself to edit it. Access rights may be set beforehand or later while viewing the information, for example. In addition, the permissible operations for a certain user can be chosen to be dependent on the authentication method used. For example, authentication by a smart card would allow the user to edit the information, but authentication by only an ID/password method would only allow the user to view the information.

1.3 Virtual smart card technology

This provides smart card functions on a server in a virtual manner. A smart card can perform various kinds of processing for the user when accessing an information system. For example, it can create a digital signature for the user or compute the user's balance after a product has been purchased. Achieving some or all of such smart card functions on a server enables the burden of providing those functions to be divided flexibly between the server and actual smart cards. This should help reduce the com-

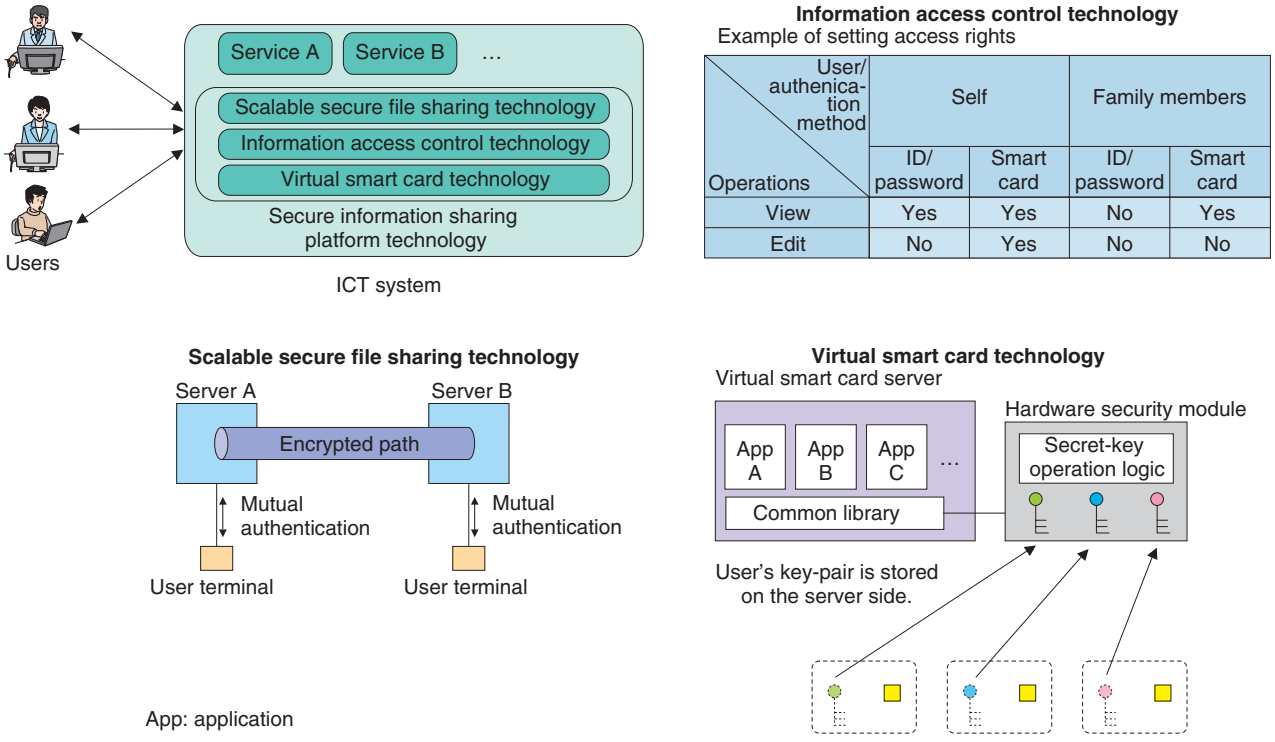

Fig. 1. Secure information sharing platform technology.

plexity of functions required on smart cards and simplify the issuing and distribution of smart cards.

Furthermore, as the user's key-pair is highly confidential information, the virtual smart card technology stores that information in a hardware security module to prevent tampering. This technology also allows applications to be added to the virtual smart card on the server as needed in a similar manner to that in actual multi-application smart cards.

2. Application to e-government

The idea behind e-government is to make the work of government more efficient and provide government services that are truly easy for the public to use through administrative mechanisms that use ICT. The need for e-government is becoming increasingly apparent, but there are a number of issues that need to be resolved before it can be truly realized. In this regard, we have studied the application of secure information sharing platform technology to the field of e-government and consider that the following issues need to be addressed for e-government implementation to be solved (**Fig. 2**).

2.1 Issue 1: Safe sharing of personal information

In e-government, a government institution must be able to deliver information pertaining to a certain person to that person in a secure manner. At the same time, a member of the public may wish to submit an application of some kind to a government institution. Performing such tasks safely over the network requires, for example, document-encryption and mutual-authentication technologies. In addition, the transfer of critical information requires a delivery certification function to enable the user to confirm that the information has indeed been delivered to the other party. To meet these requirements, we can consider the use of scalable secure file sharing technology, as described above. This can provide safe and reliable information transfer, and, if combined with virtual smart card technology, it can provide a high level of security by performing authentication and data encryption using the user's key-pair without the need to distribute high-performance smart cards equipped with PKI functions to users.

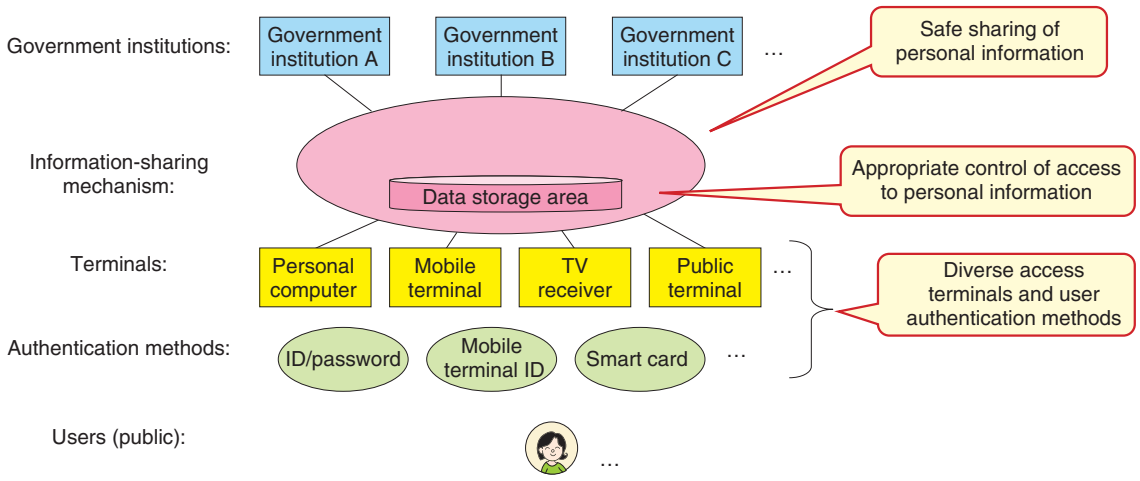

Fig. 2. Issues in e-government.

2.2 Issue 2: Appropriate control of access to personal information

In e-government, there are situations in which information related to a certain person on a server needs to be read or edited by someone other than that person. For example, a doctor may need to check a patient's health-insurance information or medical-exam history and a parent may wish to submit an application to a government institution on behalf of his or her child who is still a minor. In such situations, we can consider the use of information access control technology. This allows systematic control of who is allowed to do what to information concerning a certain individual. In this way, the abovementioned situations can be handled in e-government.

2.3 Issue 3: Diverse access terminals and user authentication methods

This issue relates to the likelihood of people wishing to access e-government services using various types of terminals and forms of access, which will have to be supported by the system. For example, we can imagine people using personal computers, mobile handsets, television sets, and terminals in public locations. We can also expect user authentication methods to be just as diverse: an ID/password method, mobile handset ID, smart card, and so on.

The smart card is commonly used as a device distributed to users for personal-authentication and digital-signature purposes, but looking forward, there will no doubt be a need for access to e-government services from terminals that cannot be equipped with a smart card reader/writer. In response to this need, we can use virtual smart card technology to create a system that allows e-government services to be received even without the use of physical smart cards.

Furthermore, as e-government continues to progress and a wide range of public and private services comes to be provided, the pressure on smart cards to become even more sophisticated and the complexity of smart card issuance and distribution may become a problem. We expect virtual smart card technology to be an effective means of avoiding this problem.

3. Prototype system

On the basis of the study described above, we developed a prototype system for an e-government platform as a system that applies secure information sharing platform technology to the field of e-government. As schematically shown in **Fig. 3**, this system consists of five subsystems: the core, virtual smart card, authentication processing, and portal sections and the information-holding institution.

3.1 Core section

As the heart of the system, this section interacts with the other subsystems and controls various processes. Using scalable secure file sharing technology, it safely and reliably exchanges information with the information-holding institution (see section 3.5). The core section is also connected to a database for storing information received from the information-hold-

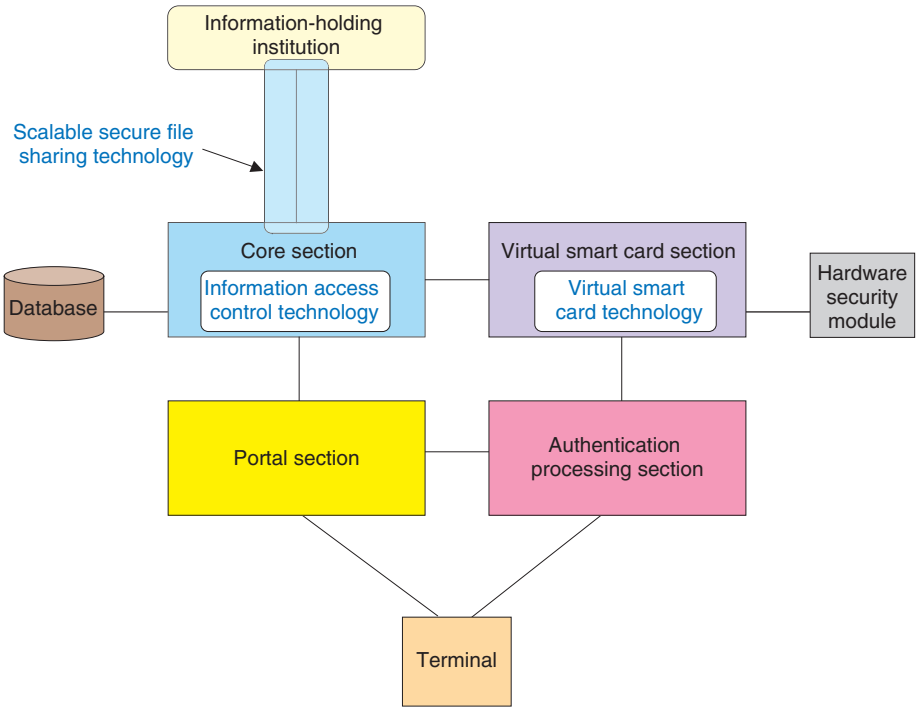

Fig. 3. Schematic of prototype for e-Government platform.

ing institution. This storage area is divided into sections, one for each user, and information access control technology is used to achieve detailed control of access to information stored in this database.

3.2 Virtual smart card section

This section uses virtual smart card technology to achieve smart card functions on a server. This section includes a hardware security module for storing users' secret keys. It receives successful user authentication results from the authentication processing section (section 3.3), generates digital signatures, and performs document decryption and other processes using the user's secret key.

3.3 Authentication processing section

This section performs user authentication. It supports two authentication methods: ID/password and smart card. Using the security assertion markup language (SAML) mechanism, it passes authentication results to the portal section (section 3.4) and the virtual smart card section.

3.4 Portal section

The portal section formats information (extensible markup language (XML) documents) sent from the information-holding institution for the user and displays that information to the user. It also has a function for accepting user applications destined for the information-holding institution. After receiving successful user-authentication results from the authentication processing section, the portal section presents the information to the user.

3.5 Information-holding institution

This corresponds to the system of government institutions for holding information pertaining to each citizen. It uses scalable secure file sharing technology to exchange information with the core section.

4. Process-flow verification

Using the prototype system described above, we executed the following three process flows on actual equipment and verified that the countermeasures for the three issues described in the previous section could be achieved (**Fig. 4**).

4.1 Viewing

In this process, the user views his or her personal

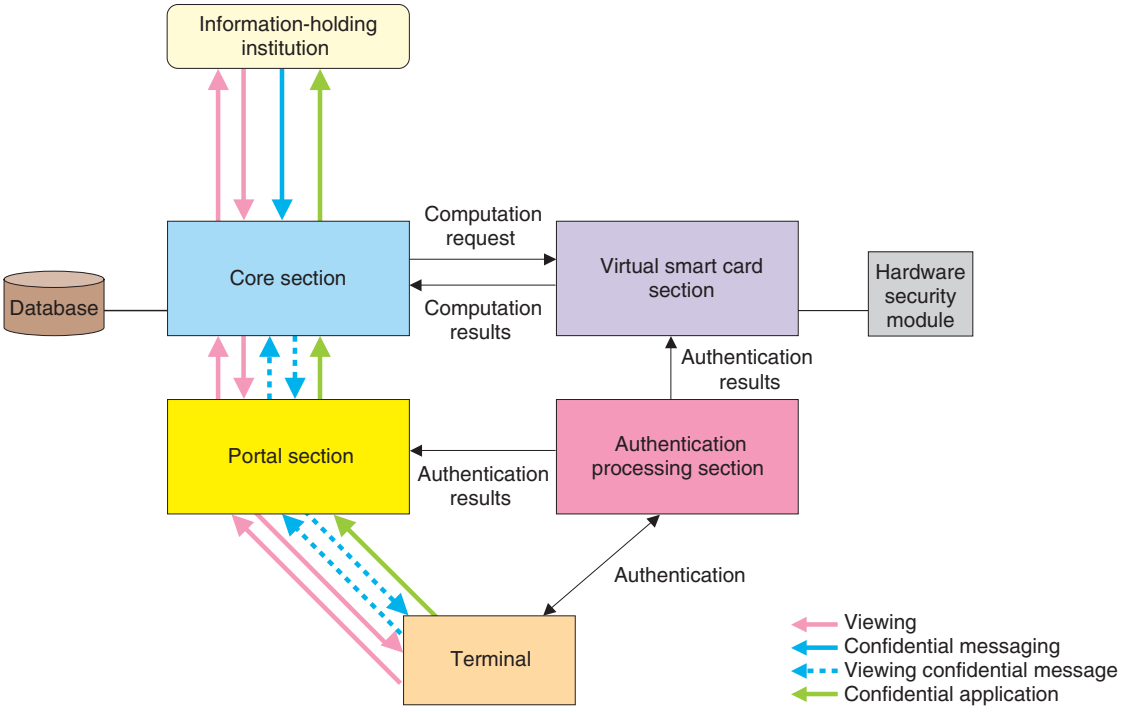

Fig. 4. Process flows.

information held by the information-holding institution. That information can be stored in the user's own data-storage area in the core section as needed.

4.2 Confidential messaging

In this process, the information-holding institution sends information about a particular user to that user. That information is encrypted using the user's public key and cannot be decrypted by anyone other than the user. To decrypt the information, this process requires the user's secret key, which is stored in the user's actual smart card or virtual smart card section on the server. The information can be stored in the user's own data-storage area in the core section as needed.

4.3 Confidential application

In this process, the user sends application information to the information-holding institution. The application information includes a digital signature generated using the user's secret key that enables any tampering with the content of the application to be detected. The user's secret key, which is stored in the user's actual smart card or virtual smart card section, is needed to attach the digital signature.

5. Concluding remarks

This article described a study on applying secure information sharing platform technology to the field of e-government and reported on the development of a prototype system for an e-government platform. In future research, we plan to use this system to investigate the scaling up of the system and backup operations and for developing techniques and systems applicable to real-life operations. We also plan to investigate the application of this technology to fields other than e-government.

References

[1] K. Yoshida, M. Tanikawa, K. Takaya, K. Morishita, and H. Fujiwara, "Scalable Secure File Sharing System," NTT Technical Review, Vol. 4, No. 10, pp. 60–65, 2006. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200610060.pdf

[2] Camellia. http://info.isl.ntt.co.jp/crypt/eng/camellia/index.html

Koji Kishi
Research Engineer, Public ICT Solution Project, NTT Service Integration Laboratories.
He received the B.A. and M.A. degrees in fundamental science from the University of Tokyo in 1994 and 1996, respectively. He joined NTT in 1996. He is currently engaged in the development of an ICT platform.

Seiji Takahashi
Research Engineer, Public ICT Solution Project, NTT Service Integration Laboratories.
He received the B.E. and M.E. degrees in information engineering from Ehime University in 1997 and 1999, respectively. He joined NTT Service Integration Laboratories in 1999 and studied electronic bidding systems. He is currently studying e-government infrastructure systems.

Kenji Murai
Deputy Manager, Network Solutions Business Unit, Business Solutions Sector, NTT DATA Corporation.
He received the B.A. degree in environmental information from Keio University, Kanagawa, in 1995. He joined NTT in 1995. He is currently working on designing and building enterprise networks.

Takumi Kashiwagi
Research Engineer, Public ICT Solution Project, NTT Service Integration Laboratories.
He received the B.E. degree in electrical and electronics engineering from Sophia University, Tokyo, in 1997. He joined NTT in 1997. He is currently engaged in the development of an ICT platform.

Yoshihiro Yoshida
Senior Research Engineer, Public ICT Solution Project, NTT Service Integration Laboratories.
He received the B.E. degree in industrial management engineering from Osaka Prefecture University in 1991. He joined NTT Information and Communication Systems Laboratories in 1991. He has been engaged in R&D of ICT platforms, security platforms, and so on.

Hirofumi Abe
Engineer, Application Platform SE Project, NTT Information Sharing Platform Laboratories.
He received the B.E. and M.E. degrees from the Faculty of Instrumentation Engineering, Keio University, Kanagawa, in 1994 and 1996, respectively. He joined NTT in 1996 and is currently engaged in the development of an information security platform.

Takashi Ikeda
Engineer, Application Platform SE Project, NTT Information Sharing Platform Laboratories.
He received the B.E. and M.E. degrees from the Faculty of Instrumentation Engineering, Keio University, Kanagawa, in 1998 and 2000, respectively. He joined NTT in 2000 and is currently engaged in the development of an information security platform.