Security Device Management Platform

Takeya Takeda† *, Koji Kishi, Keizo Murakami, Hiroki Kawamoto, and Shoko Nishida*

Abstract

NTT Service Integration Laboratories has developed a security device management platform that includes functionality for issuing smart cards, adding applications to cards after they have been issued, issuing temporary cards when a smart card is lost, and linking with external systems. The platform can support the management of smart cards and other tamper-resistant security devices in a wide range of operational scenarios.

1. Introduction

Security and personal authentication have recently become increasingly important in enterprise, academia, and the public sector. The variety of tamper-resistant security devices used for personal authentication also continues to increase: it currently includes SD (secure digital) cards that incorporate an integrated circuit (IC) chip, mobile phones with a subscriber identity module (SIM) card, and other devices in addition to conventional smart cards.

NTT Service Integration Laboratories has developed the Security Device Management (SDM) platform for centralized management of this diverse range of tamper-resistant security devices. The platform enables efficient management and operation of a safe and secure societal infrastructure that uses these tamper-resistant security devices, including configuration and updating of personal identification and authentication information and addition and removal of applications. This platform is expected to be used to generate new business and as a replacement for the Network-based IC Card Environment (NICE) [1]–[3], a platform for managing smart card information that is currently in use by companies.

2. Overview

SDM is platform software that provides integrated management of tamper-resistant security devices, from device issuing through operational functions (**Fig. 1**). Its functionality can be divided into issuing functions, which gather user information for each service and configure tamper-resistant security devices so that they can be used, and operational functions, which add and remove applications from tamper-resistant security devices and manage the multiple devices of different types used by users.

(1) Gathering user information for each service

SDM provides an interface for linking with external systems. Through this interface, user information can be automatically retrieved from an external, corporate information database system. This allows user information accumulated during registration for various services in the past to be used when a tamper-resistant security device is being issued. Thus, SDM reduces the work involved in creating new user information, reduces errors in data entry, and otherwise improves the efficiency of issuing tamper-resistant security devices.

(2) Managing smart cards

SDM can manage all of the smart cards held by each user.

(3) Adding and removing applications from tamper-resistant security devices

SDM allows applications to be added or removed from tamper-resistant security devices that have already been distributed to users. Thus, applications for a variety of services such as a facility entry system, personal computer login, and cafeteria and library systems can be added to a tamper-resistant

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

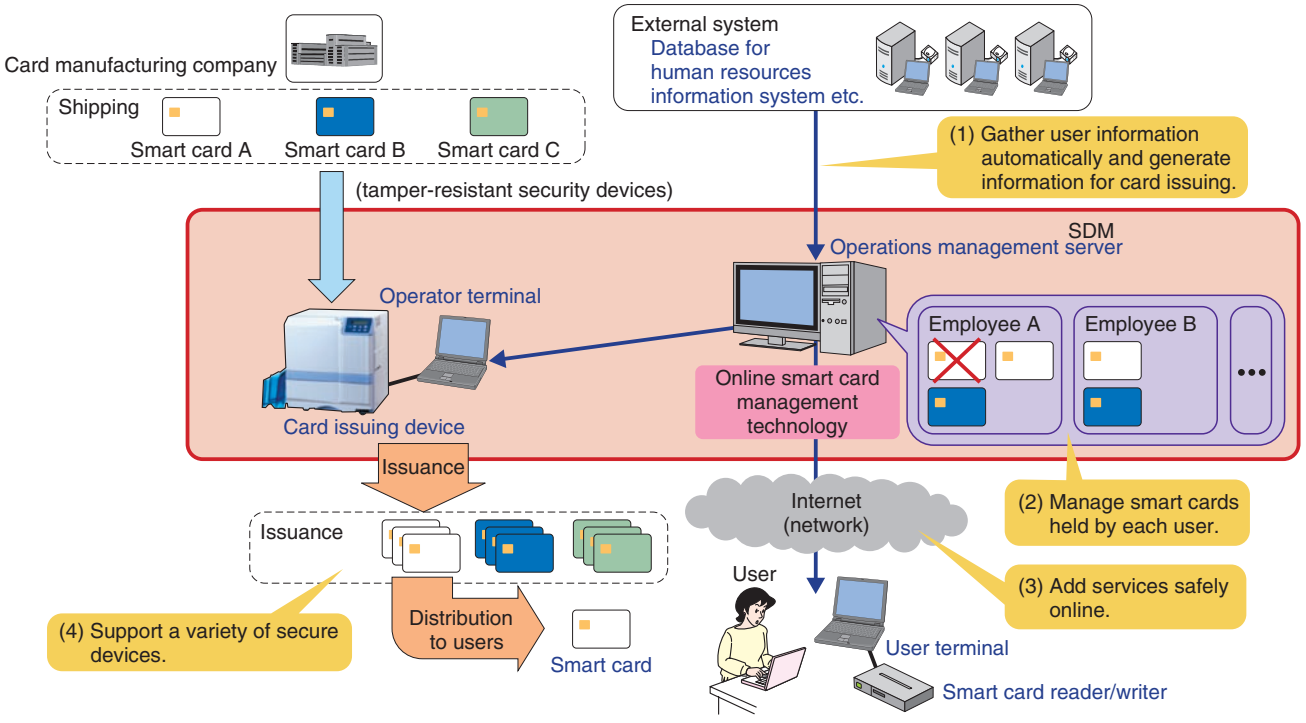


Fig. 1. Overview of SDM functionality.

security device such as a company ID (identity) card that has already been issued and distributed to employees. This allows the range of applications for the tamper-resistant security device ID to be expanded and enriched gradually.

(4) Supporting multiple tamper-resistant security devices of various types

SDM can issue and manage multiple types of devices. The functionality for managing different types of tamper-resistant security devices makes operation easier in the case of migration among tamper-resistant security devices, for example, to update a tamper-resistant security device when encryption has been compromised. The ability to manage multiple tamper-resistant security devices allows a device to be created with the same applications as the employee's original ID card; for example, a temporary ID card can be issued to an employee who has forgotten his or her ID card or the ID card can be reissued if it has been lost. Systems can thus be operated at a higher level of security and aspects such as issue numbers and expiry dates can be managed strictly.

3. Technical features

SDM is implemented as a client-server web service, so operators can perform various operations using a web terminal, such as issuing new tamper-resistant security devices or performing operational tasks. An open source framework was used, so the user interface and business logic can be customized, modified, and maintained easily.

3.1 Script for generating device issuing information

SDM is easily customizable for various solutions owing to the development of an easy scripting language called Apdu Markup Language (AML). AML makes it easy to write task rules, such as rules for generating commands to issue or operate a tamper-resistant security device or to transform data when linking with an external system (**Fig. 2**). Writing and modifying AML scripts not only makes it possible to link with external systems, but also enables systems to handle new tamper-resistant security devices, whether they are a new type of IC card or an SD or SIM card incorporating an IC chip.

3.2 User-oriented data model

SDM uses a data model to manage the number, types, and states of tamper-resistant security devices that users possess, enabling multiple tamper-resistant

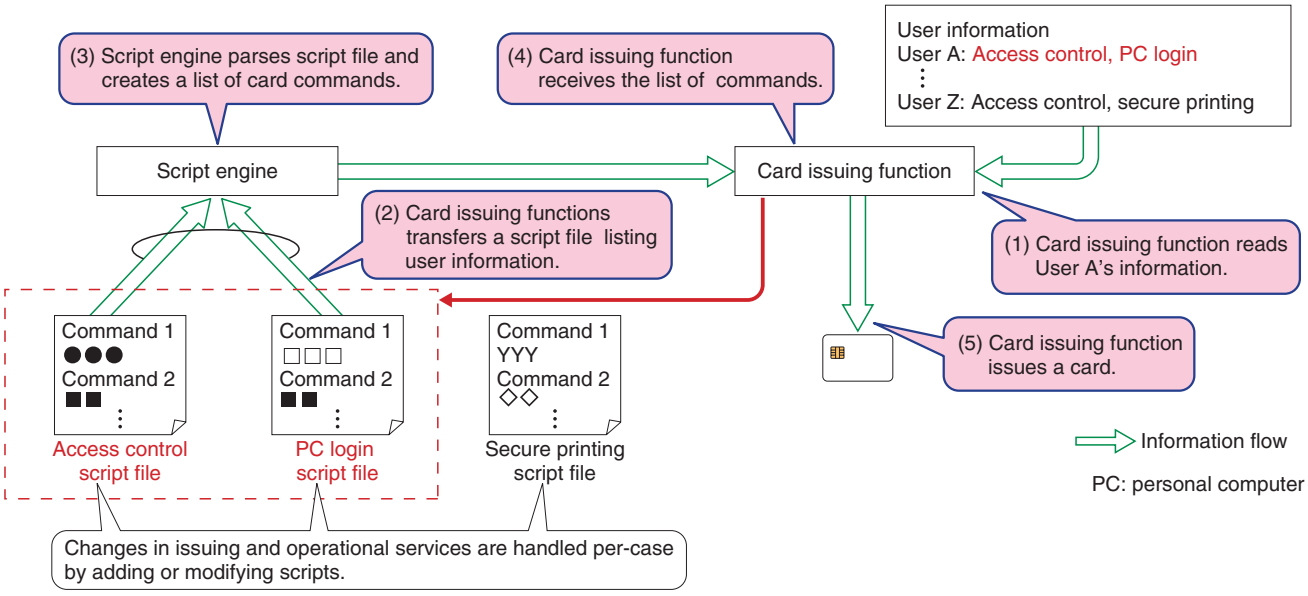


Fig. 2. Script-based generation of card issuing information.

security devices of different types to be issued and managed for each user.

3.3 Secure online tamper-resistant security device management technology adopted in the international standard

SDM can safely add services to a tamper-resistant security device over a network after the device has been issued because it uses online tamper-resistant security device management technology developed by NTT based on a public key infrastructure (PKI) and secure messaging. This technology has been recognized for its ability to add applications safely to a temper-resistant security device through its functions for flexibly managing applications on it and for flexibly handling global geographical regions, and it has been adopted in the Global Platform 2.2 international standard [4].

4. Application to system integration

The flow of a typical SDM application scenario for a company is shown in **Fig. 3** and some specific examples are described below.

(1) University student identification

When new students enter university, the information required to issue tamper-resistant security devices for all new students can be generated from student information in the registration system, and devices for all students can be created at once, by contract with a printing company, for example.

In the past, when a university spanned multiple campuses, students would have to go to another location where there was a card-issuing machine in order to add applications to their student ID card in order to use new facilities or services on another campus. SDM makes this much more convenient because applications can be added, or removed to stop a service being used, wherever there is an operator terminal. Temporary cards can be issued if a student forgets or loses an ID card, which helps prevent unauthorized use of student cards and enables the student to continue using the services on the card.

(2) Corporate identification

When an employee's employment status or location changes or the card's expiry date is approaching, information for issuing a new ID card or reissuing a new version of the existing one is generated. SDM allows the card to be issued immediately, rather than through a processed contracted out to a printing company, for example.

When an employee needs access to in-house thin-client devices or entry to secure areas, the required application can be added to his or her employee ID card. Moreover, when an employee forgets or loses an ID card, a temporary card with only the minimum applications and limited to the required use can be issued. This helps prevent abuse of ID cards and

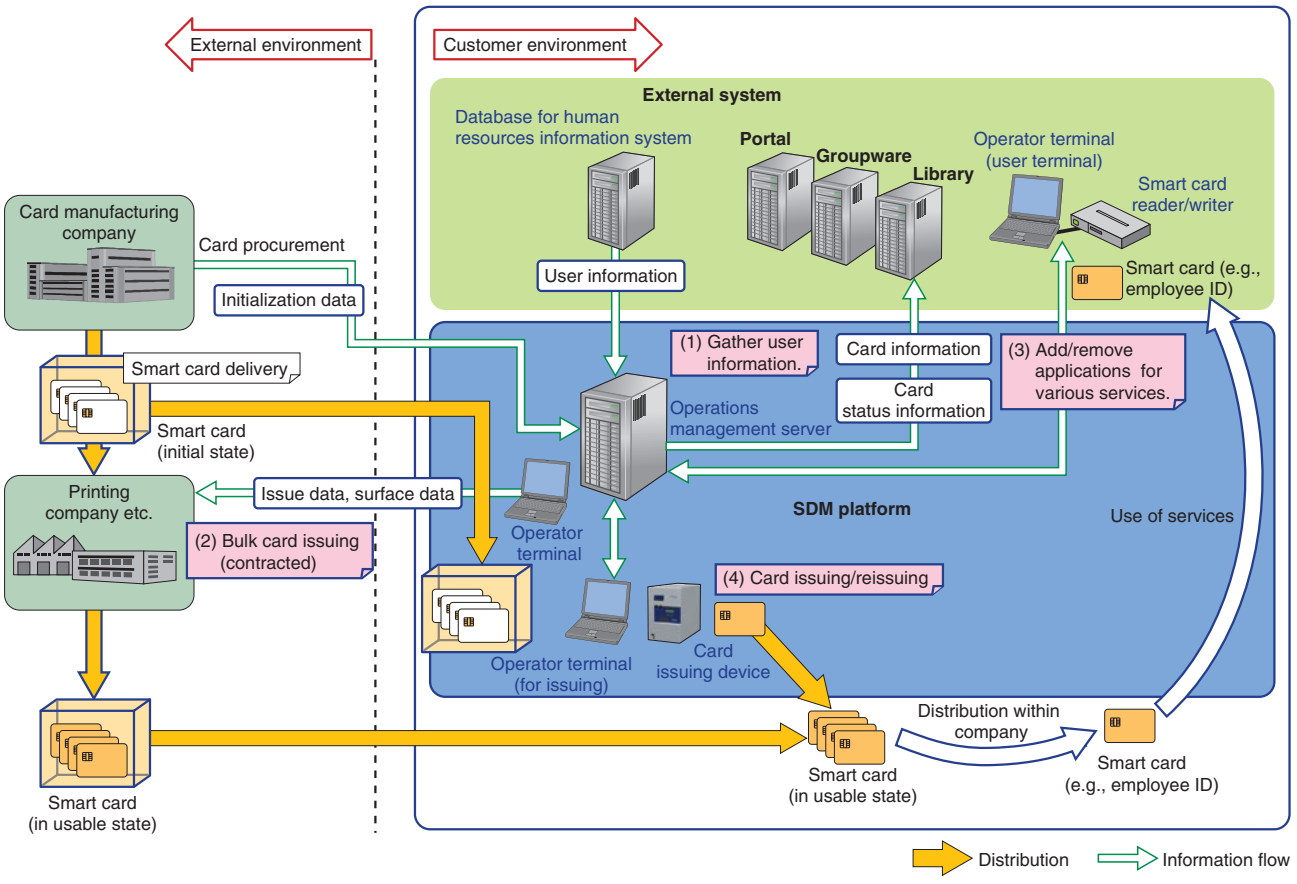


Fig. 3. SDM application scenario.

allows employees to continue to use the added services.

5. Future development

For some time, we have been working on updating and expanding existing systems such as employee and student ID cards that have been used in environments where they are relatively limited. This has included organizing and streamlining public and other external use of smart cards and extending basic functionality such as gathering user information, issuing cards, and performing other operational tasks.

We will continue to work on needs and issues selected from both domestic and global perspectives, targeting cost reductions and business continuity planning and considering general market trends such as cloud-services business and smartphones equipped with near-field communications, as well as trends toward external use in national and regional governments. As technical development advances, we will also contribute to the development of businesses that offer superior solutions for enterprises.

References

[1] S. Ijuin, T. Yamamoto, S. Hirata, K. Suzuki, Y. Wada, T. Kashiwagi, and N. Kaku, "Development of a NICE-based Smart Card System Conforming to the GlobalPlatform Specifications," NTT Technical Review, Vol. 2, No. 4, pp. 66–69, 2004. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200404066.pdf

[2] T. Kashiwagi, H. Kawamura, K. Kishi, K. Murai, and T. Yamamoto, "NICE V8.1: Smart Card Management Platform that Can Replace Compromised Encryption Schemes," NTT Technical Review, Vol. 7, No. 4, 2009. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200904le1.html

[3] Nippon Information and Communication (in Japanese). http://www.niandc.co.jp/interview/institute/no02.html

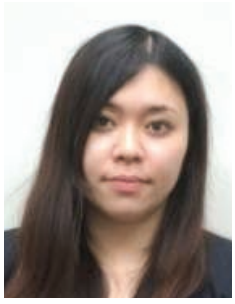
[4] GlobalPlatform. http://www.globalplatform.org/

Takeya Takeda
Senior Research Engineer, Smart Card Platform Development Project, Public ICT Solution Project, NTT Service Integration Laboratories.
He joined NTT in 1986. He was initially engaged in research studies on the e-Japan initiative and in consulting and systems engineering for the information and communications infrastructure of local governments. He is currently engaged in the development of an ICT platform.

Koji Kishi
Senior Research Engineer, Smart Card Platform Development Project, Public ICT Solution Project, NTT Service Integration Laboratories.
He received the B.A. and M.A. degrees in basic 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.

Keizo Murakami
Smart Card Platform Development Project, Public ICT Solution Project, NTT Service Integration Laboratories.
He received the bachelor's and master's degrees in pharmacy from the University of Tokyo in 2008 and 2010, respectively. He joined NTT in 2010. He is currently engaged in the development of an ICT platform.

Hiroki Kawamoto
Research Engineer, Smart Card Platform Development Project, Public ICT Solution Project, NTT Service Integration Laboratories.
He joined NTT in 1991. He was initially engaged in the development of an in-company operation system in NTT WEST. He is currently engaged in the development of an ICT platform.



Shoko Nishida
Engineer, Smart Card Platform Development Project, Public ICT Solution Project, NTT Service Integration Laboratories.
She received the B.A. degree in science education from Fukuoka University of Education in 2007 and the M.E. degree in nonlinear physics from Kyushu University in 2009. Since joining NTT Service Integration Laboratories in 2009, she has studied an ID-management system for e-government and developed an e-government system. She is a member of the Information Processing Society of Japan.