NICE V8.1: Smart Card Management Platform that Can Replace Compromised Encryption Schemes

Takumi Kashiwagi, Hiromasa Kawamura, Koji Kishi†, Kenji Murai, and Takahiro Yamamoto

Abstract

We describe improvements made to the NICE smart card management platform to ensure its continued security by replacing encryption algorithms that are expected to become compromised by 2010.

1. Introduction

Systems that use encryption techniques are being put to use in a wide range of fields such as electronic commerce (e-commerce). SSL (secure sockets layer) communication is used in online shopping sites, which have recently appeared in large numbers, including ones designed for access by mobile phone systems such as i-mode. Encryption can guarantee that data is transmitted and received in complete safety, allowing people to use these services with peace of mind.

The safety of encryption lies in the presumption that large amounts of time and money are needed to break the encryption by using computers. However, as a result of continuing developments in computer technology and codebreaking techniques, we are starting to see reports that describe how encryption algorithms that were previously thought to be safe can be broken on practical time scales. When an encryption technique becomes vulnerable in this way, it is said to be compromised. In Japan, the Information-technology Promotion Agency (IPA) [1] has identified certain encryption algorithms that can be broken with lower computational costs than originally envisaged. These algorithms have thus been categorized as being liable to become compromised [2].

One of the applications of encryption is digital signatures. When data is sent electronically, a digital signature can be generated and appended to the data to guarantee that the data was created by the person who sent it. Digital signatures are generated using hash functions that produce different results for different input data. A typical hash function used for this purpose is the SHA-1 algorithm. In 2005, it emerged that cryptography researchers had discovered a method that can be used to attack the SHA-1 algorithm. Under these circumstances, the National Institute of Standards and Technology (NIST) in the USA set out a policy for replacing all US government-standard encryption techniques that are currently used for public-key encryption, shared-key encryption, hash functions, and the like with safe encryption techniques by 2010 before any large problems develop [3].

2. NICE

2.1 Overview

In today's information technology society, data security is crucial, so smart cards are being applied to an increasingly wide range of fields. NICE is a system for the integrated operational management of smart cards, including their issue, distribution, and use. This system is widely used in various fields including community-based citizen card systems, employee/student card systems, and financial bank

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

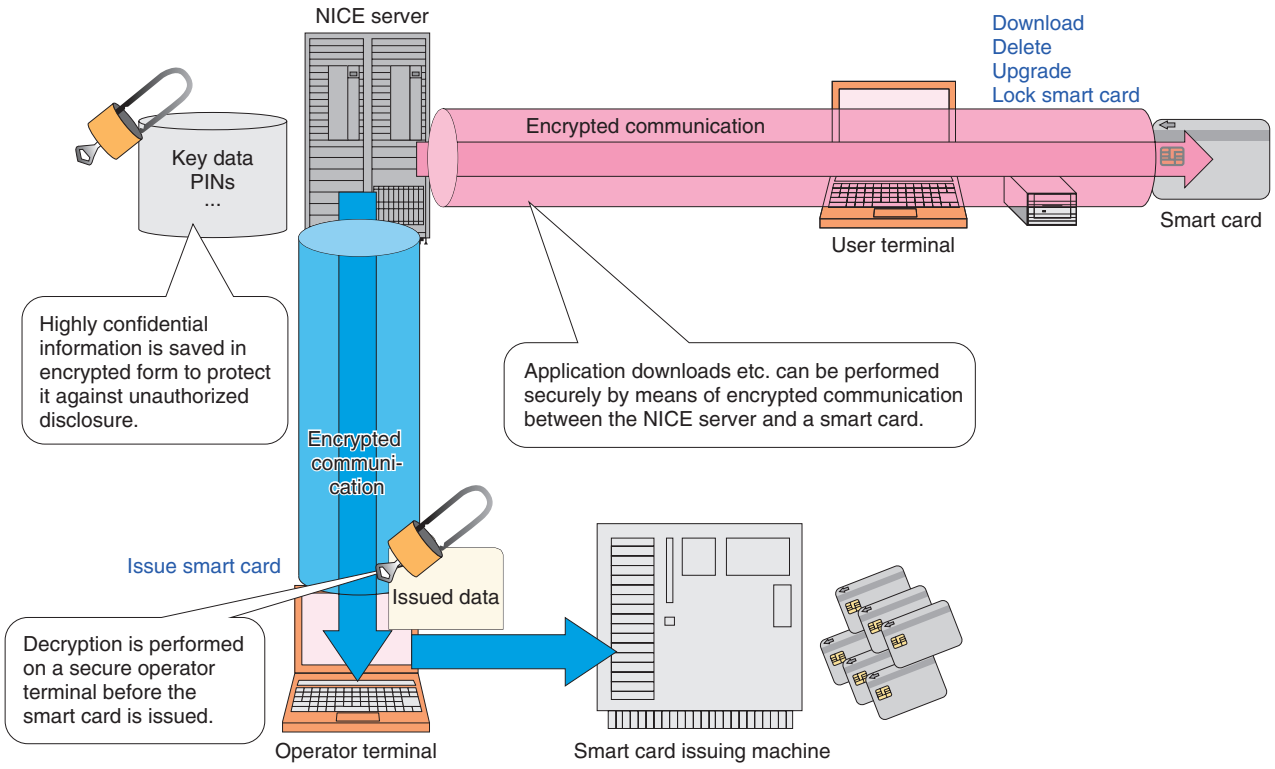

Fig. 1. Overview of NICE.

card systems [4]. An overview of NICE is shown in **Fig. 1**.

One of the features of NICE is its function for downloading new applications to users' smart cards across networks. This function is very useful for deploying new services without having to retrieve smart cards that are already in circulation. NICE also includes functions for upgrading the applications installed on smart cards and for deleting applications that are no longer needed.

NICE also allows the functions of a smart card to be remotely locked over a network if the smart card is lost or stolen, for example. When the use of a smart card is temporarily suspended, on the basis of a request from the user or for some other reason, the NICE operational management staff can set a smart card locking function so that the smart card is automatically locked the next time it is connected to NICE. The NICE system includes a range of such functions that can be used for the operational management of smart cards whenever they are used over the network.

2.2 Encryption functions

The data stored in a smart card includes highly confidential data such as key information used for encryption and personal identification numbers (PINs). To manage this data safely, a scheme was developed whereby the data is encrypted when it is stored in the NICE servers, and this data is decrypted by a secure terminal immediately before it is transmitted to the smart card issuing machine.

When a NICE server downloads, deletes, or upgrades applications on an issued smart card, the server and the smart card perform direct two-way authentication. During this authentication, a session key is generated for use in subsequent communication, and safe encrypted communication can be performed by using this key mutually between the server and the smart card. The locking and unlocking of smart cards is also performed using a similar process, thereby making it impossible for anyone to tamper with the state of a smart card by using an unauthorized terminal or server.

In this way, NICE uses encryption techniques in various different functions. To ensure their continued use in the future, it is necessary to tackle the problem

Table 1. Encryption algorithms added in NICE V8.1.

Algorithm			Main functions in NICE	Notes
Public-key encryption	Signing	ECDSA	Used when sharing keys and for two-way authentication of smart cards.	Key length used for elliptic curve encryption corresponds to 256 bits.
	Key sharing	ECDH		
Shared-key encryption	Block cipher	Camellia	Used for session keys when communicating with smart cards and for saving confidential information in the server in encrypted form.	Key length corresponds to 128 bits.
Hash function		SHA-256	Used where digital signatures are required.	—

ECDH: Elliptic Curve Diffie-Hellman

of compromised encryption, and for this purpose NICE V8.1 was developed.

3. Requirements for supplementary encryption algorithms

There are three main requirements for the encryption algorithms added in NICE V8.1. First, they should still be usable safely after 2010. Second, considering that NICE has been widely introduced into the public arena, they must be compatible with the e-Government Recommended Ciphers List* (algorithms recommended for procurement in electronic government) [5]. Third, they should be suitable for the limited resources of a smart card (memory and processing capability). Smart cards do not have the advanced processing capabilities of personal computers, so the addition of advanced encryption algorithms is liable to impair performance.

For public-key encryption, smart cards issued by NICE have hitherto used RSA encryption (named after Rivest, Shamir, and Adleman) with a key length of 1024 bits. RSA is a very widely used public key encryption algorithm, but it has been recommended that the key length should be increased to at least 2048 bits in the future. Consequently, smart cards have come to use elliptic curve encryption, which is said to provide the same level of safety as other encryption algorithms, such as RSA, but with shorter key lengths. Elliptic curve encryption, also known as elliptic curve cryptography (ECC), is an encryption technique based on the difficulty of discrete logarithm problems on elliptic curves. As a result of their favorable characteristics in terms of processing speeds and the like, they have recently been widely used in embedded systems software development.

The encryption algorithms newly added in NICE V8.1 considering these requirements are listed in **Table 1**. ECDSA (Elliptic Curve Digital Signature Algorithm) with a key length of 256 bits, which is used for public key encryption, has a strength equivalent to RSA with a key length of 3072 bits. In shared-key encryption, NICE has hitherto been compatible with 3-key TDES (triple data encryption standard), which is mentioned in the e-Government Recommended Ciphers List. However, since this became a conditional recommendation in October 2005, the Camellia encryption algorithm [6] developed by NTT and Mitsubishi was added, considering that it is expected to be still safely usable in NICE in the future. The encryption algorithms chosen for addition to NICE V8.1 are rated as having usable lifetimes beyond 2030 in a document published by NIST [7].

4. Addition of new encryption algorithms

To add new encryption algorithms to NICE, it is necessary to replace the old ones that have been used so far. Doing this involves two major operational issues:

(1) Updating key information that is compatible with smart cards that use new encryption algorithms

(2) Managing the retrieval of already issued smart cards that use old encryption algorithms and their replacement with smart cards that use new encryption algorithms

These issues will not have to be considered once NICE V8.1 has been introduced, but must be considered by most users that have already introduced NICE and are considering upgrading to NICE V8.1 in the future.

The first of these issues was resolved by developing a key updating tool. A manual updating method was

* Algorithms that have been recommended for procurement in e-Government in the CRYPTREC (Cryptography Research and Evaluation Committees) project, which is jointly promoted by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry.

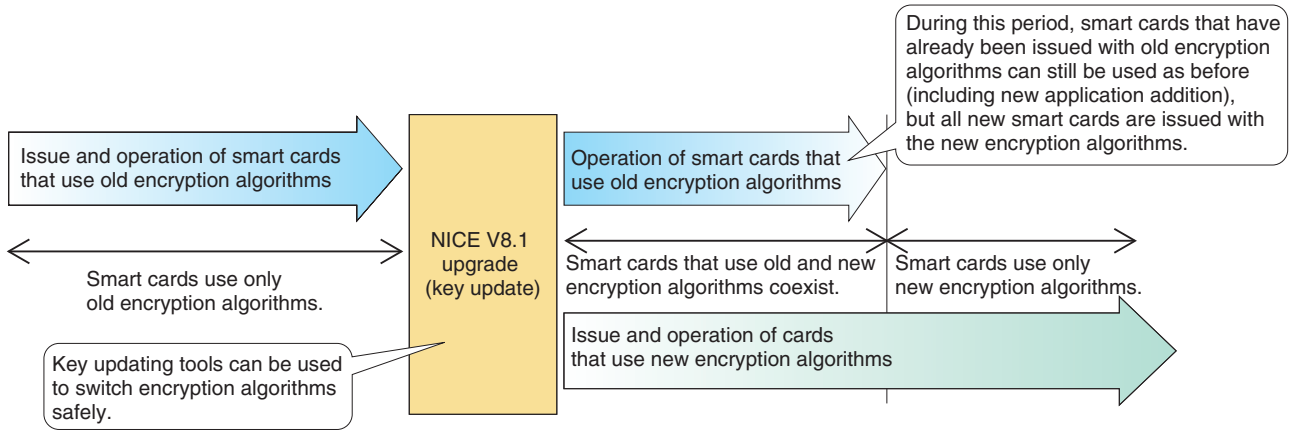

Fig. 2. Card migration plan.

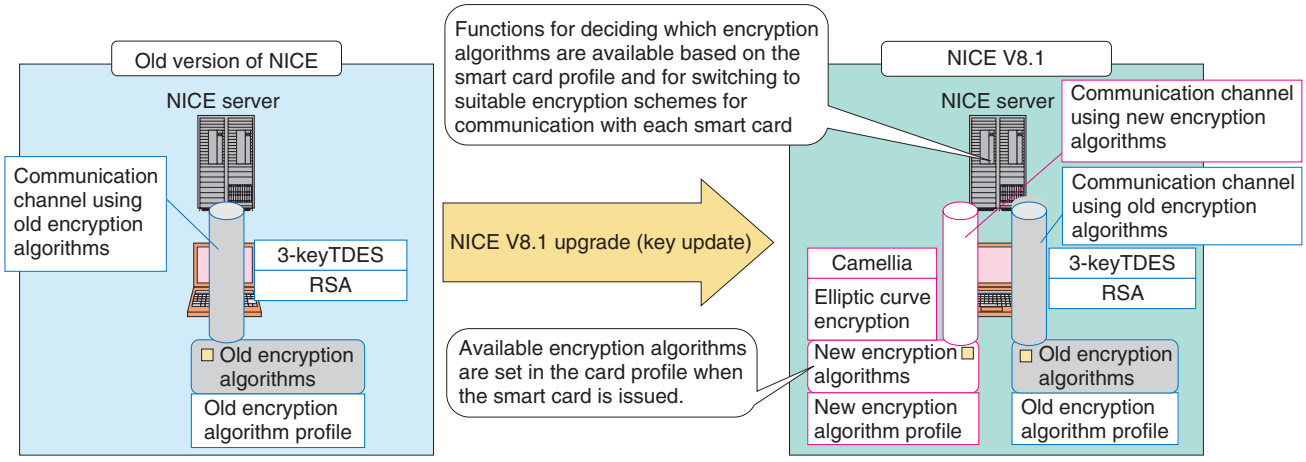

Fig. 3. Plan for using new and old encryption algorithms together.

also considered instead of a tool, but this would have had a higher risk of introducing errors when updating the key information, making it impossible not only to issue smart cards equipped with new encryption algorithms, but also to use smart cards that have already been issued. Since NICE uses encryption techniques for various different purposes, there is a large amount of key information that needs to be updated. Our tool can perform key updates safely without the risk of manual errors.

The second issue was more challenging. Retrieving all previously issued smart cards and reissuing new ones with new encryption algorithms in one go would be extremely costly. Smart cards normally have an expiry date and must be reissued every few years. They can also be reissued when they are lost, stolen, or damaged. Therefore, it was decided that in NICE V8.1, as shown in **Fig. 2**, existing smart cards will be replaced with new versions at the regular time of reissue; until that time, however, the old encryption algorithms can still be used, thereby allowing a gradual replacement schedule. To make this possible, we developed functions for setting profile information in smart cards when they are issued and for deciding which encryption algorithm to use for communication with a smart card on the basis of this profile information. NICE V8.1 can perform operational management in an environment containing a mixture of old and new smart cards by performing encryption using the algorithms supported by each type of smart

card.

Since the encryption algorithms supported by a smart card are automatically selected by the NICE server, smart card users can still perform operations such as adding and upgrading applications in the same way as before. An environment where smart cards that use new and old encryption algorithms can coexist is illustrated in **Fig. 3**.

5. Conclusion

NICE V8.1 has been developed as a system that can safely operate smart cards that use new encryption algorithms. Smart cards have become popular as highly secure portable devices, and dealing with compromised encryption is one of the most important issues for ensuring their continued success. In the future, we intend to carry on promoting the use of NICE V8.1 so that NICE can continue to be used safely not only by its existing users but also by new users.

References

[1] http://www.ipa.go.jp/about/english/index.html
[2] http://www.ipa.go.jp/security/fy16/reports/crypt_compromize/documents/crypt_compromize.pdf (in Japanese).
[3] http://www.atmarkit.co.jp/fsecurity/rensai/crypt01/crypt02.html (in Japanese).
[4] Y. Ito, M. Tanaka, J. Hashimoto, K. Murai, K. Kishi, S. Hirata, T. Yamamoto, and S. Ijuin, "Simplifying the Construction and Operation of Smart Card Systems: NICE V4.1," NTT Technical Review, Vol. 2, No. 5, pp. 35–39, 2004. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200405035.pdf
[5] http://www.cryptrec.go.jp/list.html (in Japanese).
[6] M. Kanda, "Promoting the Use of Camellia," NTT Technical Review, Vol. 4, No. 2, pp. 49–53, 2006. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200602049.pdf
[7] http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf

Takumi Kashiwagi
Member, Smartcard Service Promotion 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 ID management platform.

Hiromasa Kawamura
Member, Smartcard Service Promotion Project, NTT Service Integration Laboratories.
He received the B.E. and M.E. degrees in electrical engineering from Tokushima University, in 1984 and 1986, respectively. He joined NTT in 1986. He is currently engaged in the development of an ID management platform.

Koji Kishi
Member, Smartcard Service Promotion Project, NTT Service Integration Laboratories.
He received the B.A. and M.A. degrees in fundamental science from Tokyo University, in 1994 and 1996, respectively. He joined NTT in 1996. He is currently engaged in the development of an ID management platform.

Kenji Murai
Member, Smartcard Service Promotion Project, NTT Service Integration Laboratories.
He received the B.A. degree in environmental information from Keio University, Kanagawa, in 1995. He joined NTT in 1995. He is engaged in the development of an ID management platform.

Takahiro Yamamoto
Senior Research Engineer, Supervisor, Smartcard Service Promotion Project, NTT Service Integration Laboratories.
He received the B.E. degree in electrical engineering and the M.E. degree in information engineering from Nagoya University, Aichi, in 1987 and 1989, respectively. He joined NTT in 1989. He is currently engaged in the development of an ID management platform.