Technology Reports

TENeT—Specifications for Realizing a Safe Electronic Voucher Trading Market

Masayuki Terada, Kensaku Mori and Sadayuki Hongo

In the spring of 2006, groups of TENeT specifications for safe electronic voucher trading services, were standardized in the T-Engine Forum. This article describes new smart card communication architecture, which is a technology for realizing safe electronic voucher trading market.

1. Introduction

We have worked on R&D of technologies for trading electronic vouchers (for example, various loyalty/award points and coupons, tickets, content reproduction rights, and the like) safely between users. With these technologies, it is possible to implement a safe electronic market service in which users can securely and fairly buy, sell, or exchange electronic vouchers among themselves using their mobile terminals [1][2].

To support rapid deployment of the safe electronic market service described above, we have developed and standardized the specifications of a framework for such a service within the T-Engine Forum, which is the standardization workgroup to promote the T-Engine as an open, standardized development platform for embedded systems. The specifications were published by the T-Engine Forum as a series of standard specifications in the spring of 2006 [3]-[7]. These specifications are hereinafter collectively referred to as Trusted Environment with Networking eTRON (TENeT)[*1] specifications.

One of the main design objectives of the TENeT specifications is that each Application Program (AP) for realizing an electronic market service can be stored easily and efficiently on a mobile terminal having a smart card slot (such as a mobile terminal with a SIM/UIM[*2] slot). In order to achieve this objective,

[*1] eTRON: Security infrastructure for constructing a ubiquitous environment being developed mainly by the T-Engine Forum, which aims to realize an "electronic entity" of electronic information being difficult to copy or modify, thus facilitating secure distribution of electronic information among information equipment.

in association with the University of Tokyo, we have established a new smart card communication architecture that supports distributed processing (electronic voucher trading and so on) on multiple smart cards networked together.

This article describes the purposes of determining the specifications, examples of the services that can be realized by the specifications, the design objectives, an overview of realization technologies, an overview of prototype bundling simultaneously performed while determining the specifications, and evaluation results.

2. Objectives of Defining Specifications

The T-Engine Forum is a standardization group to realize a ubiquitous computing environment where everything has a computer incorporated in it and is connected to a network. Several specifications for embedded systems[*3] including T-Kernel[*4], the successor to the Industrial TRON Operating System (ITRON OS)[*5] which has a large share of the operating systems for embedded systems, and eTRON, which provides a tamper-resistant capability[*6] to embedded systems [3] have been defined by the T-Engine Forum. The TENeT specifications have been established by adding significant expansions to the eTRON specifications, in order to easily and efficiently construct a service which trades safely and utilizes electronic vouchers on mobile terminals.

Figure 1 shows an example of the service that can be realized with the present specifications. Each user holds a mobile terminal and a smart card implementing the TENeT specifications. Users can securely and fairly buy, sell, or exchange electronic vouchers through a network via these mobile terminals.

3. Design Goals and Problems

As design goals of the TENeT specifications for realizing a ubiquitous computing environment, the following four items have been defined:

1) the ability to handle various electronic vouchers uniformly;
2) the ability to guarantee fair trades, i.e., payment must not be committed without receiving the merchandise purchased as

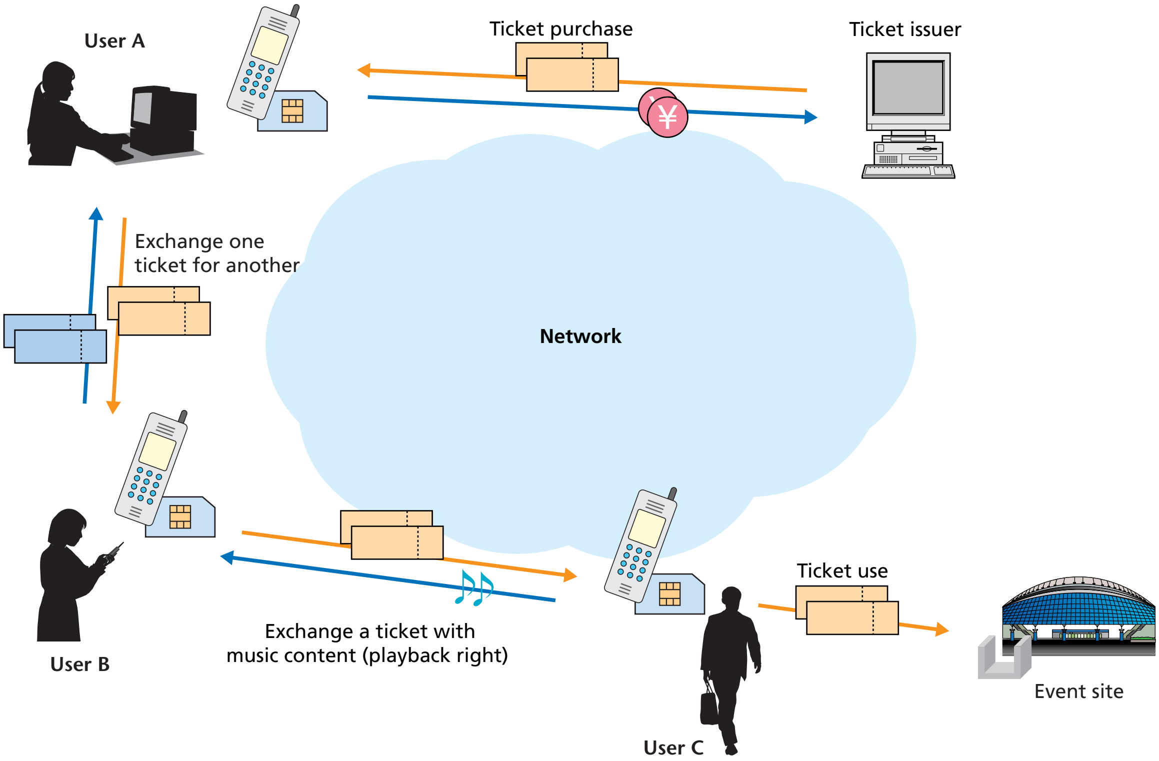

User A
Ticket purchase
Ticket issuer
¥
Exchange one ticket for another
Network
User B
Exchange a ticket with music content (playback right)
Ticket use
Event site
User C

Figure 1 Service image realized by the TENeT specifications

*2 UIM: A smart card that stores subscriber information such as a telephone number. It is inserted into the mobile terminal to identify the user. A FOMA card is an example of UIM.

*3 Embedded system: Equipment with built-in software and a CPU used for a specific applications such as Personal Digital Assistant (PDA) and home appliances.

*4 T-Kernel: One of the standards of real-time operating systems developed based on the ITRON technologies, with which dynamic control functions and various resources are being expanded.

*5 ITRON OS: One of the standards of real-time operating systems for embedded systems, widely adopted as an OS of Second-Generation mobile terminals.

*6 Tamper-resistant capability: A property to prevent integrated programs, data, and other digital information from unauthorized referencing or rewriting.

well as merchandise must not be sent without payments;

3) to provide interfaces for easy construction of APs which utilize the TENeT specifications; and
4) to provide compact and efficient implementation, enough to be feasibly implemented on devices with limited resources such as smart cards and mobile phones.

Among the above items, objectives 1) and 2) have been accomplished by establishing and implementing a technology, namely "an optimistic fair exchange protocol for trading electronic rights" [2].

This protocol assumes that the protocol will be implemented as the distributed protocol among smart cards. However, because conventional smart card interface designs such as ISO 7816 have not considered a utilization method for mutual communications between multiple smart cards, a problem is generated in that constructing APs becomes complicated when the protocol is implemented using these specifications.

For example, ISO 7816-4 [8] that defines the command formats exchanged with smart cards in ISO 7816, provides only closed, simple access methods between a host (a device that uses a smart card) and a smart card where a command is sent from a host to a smart card, and subsequently the smart card sends back the result of processing the received command to the host (**Figure 2**). By using this method to realize a distributed protocol between smart cards, it is necessary for an AP on each mobile terminal to convert every message to be exchanged into a number of suitable commands. This causes the structure and implementation of the AP to become complicated, and also makes the above objectives 3) and 4) difficult to accomplish (**Figure 3**).

4. Technology Overview

In order to solve the problems described in the previous section and to accomplish objectives 3) and 4), we developed a framework based on a new paradigm where smart cards autonomously exchange messages with one another without APs relaying the exchanged messages [9][10]. An architecture based on this technology has been adopted by the TENeT specifications.

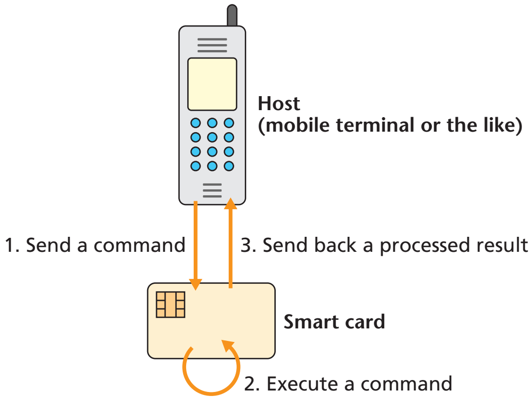

Host
(mobile terminal or the like)
1. Send a command
3. Send back a processed result
Smart card
2. Execute a command

Figure 2 Smart card processing flow using ISO 7816-4

Since the messages of the exchange protocol for electronic vouchers are transferred among smart cards without APs relaying messages, it is possible to construct an AP without being aware of the details of the protocol including the transmission and reception steps involved as well as the contents of those messages (**Figure 4**).

4.1 Message Structure

In the TENeT specifications, a message exchanged between an AP and a smart card is called an extended eTRON Protocol (e^2TP) message, which is represented by packets of four data: *src*, *dst*, *mtype*, *param*; *src* and *dst* represent the source and destination of the message, respectively; *mtype* represents the code specifying the message of the *param* (e.g., codes represent "Generation of an electronic voucher," "Start exchanging an electronic voucher," etc.); and *param* is a set of parameters describing the message specified by *mtype* (e.g., the content of the electronic voucher to be generated, in the case of "Generation of an electronic voucher").

For example, a message instructing the generation of an electronic voucher from an AP having the identifier A1 to a smart card having the identifier C1 becomes (A1, C1, 0x0102, <Content of the electronic voucher to be generated>). Here, 0x0102 is the hexadecimal notation of the message type code instructing to generate an electronic voucher.

Details of the structure of the e^2TP message described above

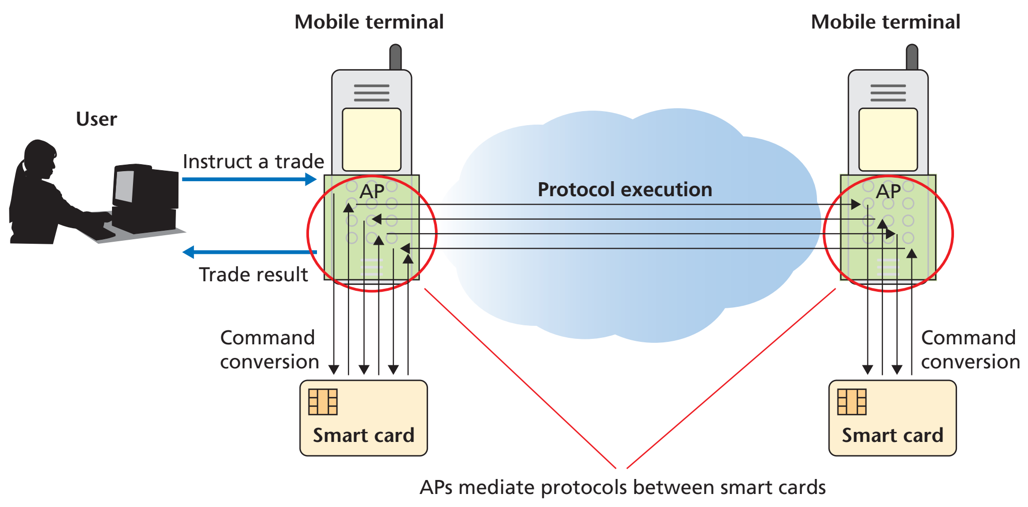


Figure 3 Protocol execution between smart cards in conventional smart card communication architecture

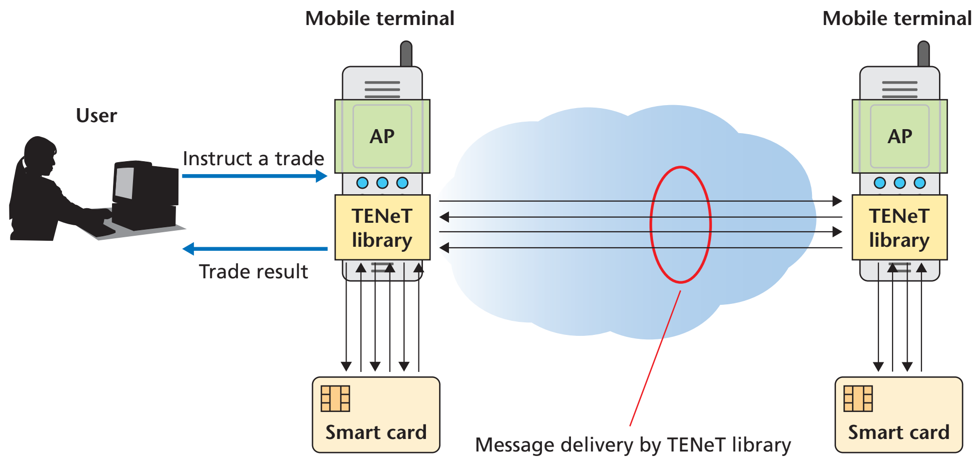


Figure 4 Protocol execution between smart cards by TENeT

are defined in "e^2TP Message Specifications" [3] and the message type codes and parameters for each message type are defined in "TENeT Message Specifications" [5].

4.2 Message Delivery Method

The Messaging library[*7] in TENeT performs the delivery of messages from APs by providing a means of exchanging messages between APs and smart cards. When an AP sends a message, the messaging library writes the message into a shared memory area called a dispatch table. Similarly, a message sent from a smart card is written into the dispatch table by a program module called a "smart card proxy." A message transmitted from another mobile terminal is written into the dispatch table by a program module called the "remote proxy" (**Figure 5**).

An AP receives a message by registering a handler[*8] in the messaging library, which provides notification of the arrival of a message addressed to this AP. This handler is invoked when a message addressed to the AP is written into the dispatch table, and notifies the AP of the arrival of the message.

A similar handler is provided to each smart card proxy and remote proxy, and is invoked when a message addressed to that smart card or another mobile terminal is registered. The smart card proxy sends the message obtained by the handler to the smart card as is, and the remote proxy sends the message to the other mobile terminal through a network.

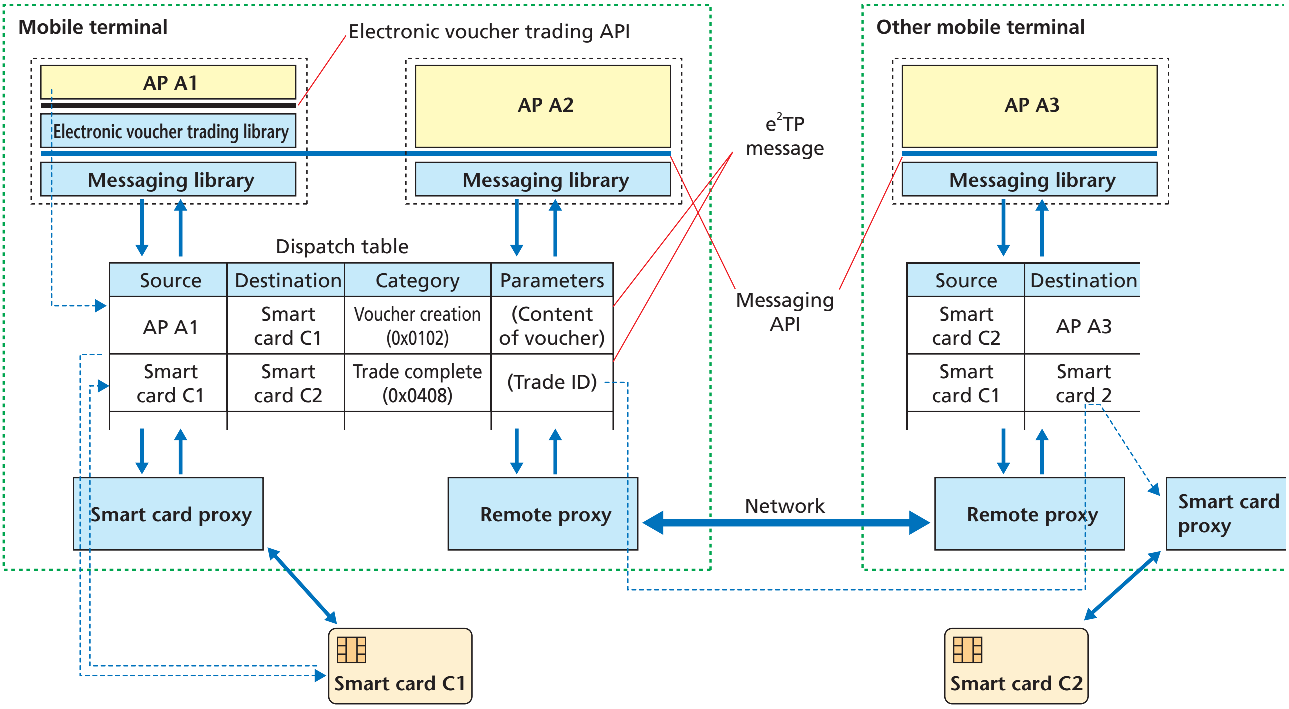
In this way, since each message is autonomously delivered by the messaging library without APs mediating messages, the burden of APs that require distributed communications among smart cards is significantly reduced. Furthermore, operations of the messaging library or each program proxy are executed independently without using APs or smart cards. Therefore, developers can implement APs and smart card programs without being aware of these message delivery mechanisms.

Details of the functions and interfaces provided to an AP for utilizing this message delivery mechanism are defined in "e^2TP messaging Application Program Interface (API)[*9] specifications" [6].

[*7] Library: A collection of general purpose software programs in a reusable form.

[*8] Handler: A processing routine (program) triggered by the occurrence of an event. For example, a processing routine triggered by the occurrence of a message is referred to as a message handler, and a processing routine triggered by the occurrence of an external interrupt is referred to as an interrupt handler.

[*9] API: An interface allowing upper-level software to use functions provided by the OS, middleware, etc.



Source	Destination	Category	Parameters
AP A1	Smart card C1	Voucher creation (0x0102)	(Content of voucher)
Smart card C1	Smart card C2	Trade complete (0x0408)	(Trade ID)

Source	Destination
Smart card C2	AP A3
Smart card C1	Smart card 2

Figure 5 TENeT architecture

4.3 Electronic Voucher Trading Library

Due to the message delivery mechanism described in the previous section, an AP is not required to be aware of details of the protocol executed between smart cards. As a result, the burden of constructing an AP is significantly reduced. However, in order to construct an AP by directly utilizing the messaging library, the AP is required to generate and to interpret e^2TP messages. In addition, when exception handling is required against abnormalities, such as an interruption of protocol caused by disrupted communications, it is necessary to provide a function for monitoring execution states of the protocol between smart cards.

In order to automate generation and interpretation of the e^2TP message and to enable monitoring of the execution states of the protocol if necessary from an AP, a library called the “electronic voucher trading library” is provided in TENeT. This library is positioned in the upper layer of the messaging library, and provides objects[*10] that represent the items and participants involved in trades, such as the electronic vouchers stored in a smart card, the trading partner, the execution state of the trade, and so on. The functions necessary for trades such as generating the electronic voucher, starting a trade, verifying a trading state, etc., are realized as methods provided by those objects.

This library covers almost all functions for electronic voucher trading provided by a smart card complying with the TENeT specifications; APs for trading electronic vouchers, such as an electronic wallet, can be constructed by using only the functions provided by this library. That is, developers for these APs are not required to be aware of various specifications other than the APIs provided by this library.

Details of the functions and interfaces provided by this library are defined in the “Electronic Voucher Trading API Specifications” [7].

5. Prototype Evaluation

When determining the groups of TENeT specifications, implementation feasibility and performances were verified concurrently through prototype implementations of smart cards and each library.

Considering the mid-range smart card several years in the

[*10] Object: An entity expressing a concept existing in the real world so as to enable handling in a software program. Objects are expressed as a combination of data, which indicate attributes of an entity to be expressed, and an operation to be performed with the entity.

future, a prototype smart card was implemented using a commercial smart card that has relatively high performance at the present (32-bit CPU, clock speed: 66 MHz, EEPROM: 400 KB, RAM: 16 KB). With this configuration, processing time from the starting of a trade to completion was about one second. This result shows that the specifications can be implemented with sufficient performance even by using commercial smart cards currently available.

By considering implementing in the mobile terminal, prototypes of the library were produced using Java Wireless Toolkit 2.2, which is a J2ME™ MIDP 2.0 simulator (Java2 Micro Edition[*11]; Mobile Information Device Profile[*12]). The libraries were added to the J2ME environment on the simulator as Java ARchive (JAR)[*13] files and a trading AP for verification tests was packaged as a MIDlet[*14]. As a result of implementation, the size of the message communication mechanism (including messaging library and proxies) was 45 KB and the size of the electronic voucher trading library was 99 KB (each the size of a JAR file). This combined size should not cause severe implementation problems on current mobile terminals. In addition, the resultant overhead from delivering messages under the simulation environment was less than 10 ms per message, which was almost negligible.

6. Conclusion

This article has described the TENeT specifications for realizing a safe electronic voucher trading market using a mobile terminal. We described design objectives as well as an overview of a key technology to implement the specifications, which enables us to perform distributed inter-smart card communications quite easily. By producing prototypes according to the specifications using commercially available smart cards and a J2ME simulator environment, the feasibility and performance have been evaluated. The evaluation result shows that the framework and APs based on the TENeT specifications can be feasibly implemented even by using currently available smart cards, without incurring expensive performance overheads.

REFERENCES

[1] M. Terada, M. Iguchi, M. Hanadate and K. Fujimura: "An Optimistic Protocol for Trading Electronic Rights," Proc. 6th intl. conf. Smart Card Research and Advanced Applications (CARDIS' 04), 2004.

[2] M. Terada et al.: "Fair Electronic Voucher Exchange Technology for Mobile Terminals," NTT DoCoMo Technical Journal, Vol. 7, No. 3, pp. 11–15, Oct. 2005.

[3] T-Engine Forum; http://www.t-engine.org/

[4] T-Engine Forum; "e^2TP Message Specifications," 2006.

[5] T-Engine Forum; "TENeT Message Specifications," 2006.

[6] T-Engine Forum; "e^2TP Message API Specifications," 2006.

[7] T-Engine Forum; "Electronic Voucher Trading API Specifications," 2006.

[8] ISO/IEC: "Integrated circuit(s) cards with contacts–Part 4: Interindustry commands for interchange," ISO/IEC 7816-4:1995 (E), 1995.

[9] M. Terada, K. Mori, K. Ishii, S. Hongo, T. Usaka, N. Koshizuka and K. Sakamura: "TENeT: A Framework for Distributed Smartcard," Proc. 2nd intl. conf. Security in Pervasive Computing (SPC2005), LNCS 3450, 2005.

[10] M. Terada, K. Mori, K. Ishii, S. Hongo, T. Usaka, N. Koshizuka and K. Sakamura: "A Framework for Distributed Inter-smartcard Communication," IPSJ Journal, Vol. 47, No. 2, Feb. 2006.

[*11] J2ME™: One of the Java language sets, with restrained consumption resources so as to be intended for embedded systems.
J2ME and all of the other Java-related trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

[*12] MIDP: One of the J2ME profiles. Specifications of a Java execution environment defined for a hand-held terminal, such as a mobile terminal.

[*13] JAR: A file type in which Java byte code files that have been generated by compiling Java source codes are combined into one archived file.

[*14] MIDlet: One of the Java program formats, which is downloadable through a network and capable of operating in the MIDP environment.