TENeT OUTLINE

Ver. 1.0

TEF950-S000-01.00.00/en

2005/03

T-Engine Forum

CONTENTS

1 Introduction

1.1 Purpose of this document

This document explains the purpose and characteristics of the TENeT (Trusted Environment with Networking eTRON) specification that provide Java APIs and message formats among smartcards and application programs for authority value （electronic voucher）transaction. This specification is one of the 'eTRON appliance' specifications for authority value circulation in the mobile environment.

1.2 TENeT outline

The advancement of authority value trading technology and the spread of networks as social bases in recent years has led the continued offering of services that electronically issue and use authority values, such as money and tickets. Though the types of electronic authority values being handled today are limited, it is projected in the future that, as authority value circulation services infiltrate modern society, individual information, such as personal identity certificates, will become widely distributed and a transaction market for authority values between users, such as through auctions, will appear. Figure 1 provides an image of the TENeT-based authority value transaction environment

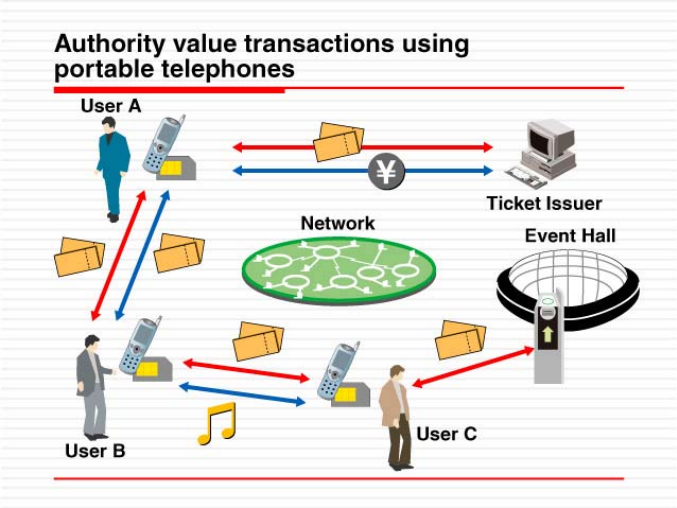

Figure 1 TENeT image

The infiltration of authority value circulation services, however, will be accompanied by risks of a proliferation of illegal acts such as altering or forging authority values Technology protecting authority values from illegal operation will be required for the development of authority value circulation framework.

Besides protecting authority values, it will also be important to assure that transactions can be done fairly, for users to securely circulate and trade authority values. In other words, when authority values are bought and sold among users for example, such illegal behavior as absconding with the authority values must be prevented. Particularly in wireless environments, such as with cell-phones, assuring transaction fairness will be an extremely important element, given that interruptions can occur in mid-transaction, due to such incidents as network cut-offs and cell-phone charge depletion.

TENeT provides means to assume transaction fairness and thus enabling users to trade authority values without risks of illegal behaviors such as absconding.

1.3 Prescribed scope of the TENeT specifications

Each of the following TENeT specifications has been prescribed to enable the mutual operability of the IC cards [M1]and application programs that make authority value transactions possible.

- TENeT authority value transaction API specification
  An API for managing and circulating IC card authority values from application programs
- TENeT messaging API specification
  An API for sending and receiving e2TP messages from application programs
- e^2TP (Extended eTRON Transfer Protocol) message specification
  Message format for e^2TP messages and mapping method for the ISO7816-4 ADPU
- TENeT message specification
  Message set for e^2TP messages that must be provided by the TENeT specification IC card.

1.4 Composition of the document

This document is composed as follows. Chapter 2 indicates the specific usage scenarios for the TENeT specifications and Chapter 3 enumerates prerequisites for the practical realization of a usage scenario. Chapter 4 outlines the TENeT specifications.

2. TENeT usage scenarios

2.1 Usage scenarios

A mobile environment is defined as “an environment where each user equips its own mobile terminal that is capable of network connection.” A typical example of the mobile terminal is a cell-phone. Authority value circulation in the mobile environment offers the following characteristics compared with authority value circulation where only a tamper-proof device such as an IC card is carried.

- The use of portable terminal network functions makes possible authority value interchanges with other users
- The use of a portable terminal user interface makes it possible to control the authority values within an owned tamper-proof device.

The usage scenarios indicated in Table 1 are conceivable through an authority value circulation in a mobile environment thanks to the above characteristics.

Table 1 Usage scenarios of authority value circulation in a mobile environment

Usage scenario	Details
Purchase of authority values	Commuter passes or tickets purchased at specific locations, such as ticket vending machines at ticket gates, and charges for electronic money can be made anytime, anywhere using the portable terminal network function.
Transfer of authority values	It transfers authority values to other users. Though specialized equipment, PCs connected to networks, and the like were required for transfers in the past, authority values can be transferred through the use of portable terminal network functions, without the need for other equipment.
Exchange of authority values	It exchanges the authority value with other users. It can mutually transfer authority values using the network function of the portable terminals, the same as indicated above. Transaction services as a whole can be applied, provided that the exchange can be executed securely. Unrestricted transaction services are possible, through free markets on networks, for example.
Use of authority values	Authority values can be used at ticket examination points and gates, by holding them over a portable terminal, in the same manner as conventional proximity type non-contact IC cards. The local communication function of portable terminals could, for example, be used in much the same way as the smart keys of automobiles to open doors automatically using authority values.

The TENeT specifications stipulate the API to be used by applications on portable terminals and the IC card input/ output messages for enabling the usage scenarios mentioned in section 2.1. From Chapter 3, we will explain the prerequisites for authority value circulation and the TENeT functions that meet these prerequisites.

3. Prerequisites for authority value circulation

In this chapter, we will categorize the prerequisites for authority value circulation that will bring about usage scenarios discussed in Chapter 2.

The authority values that enable usage scenarios are referred to as 'electronic vouchers' in RFC3506, which defines the necessary conditions that must be met [RFC3506]. Figure 2 breaks down the prerequisites to be met by the authority values, according to RFC3506 and documents [TKHF00] serving as its technical background.

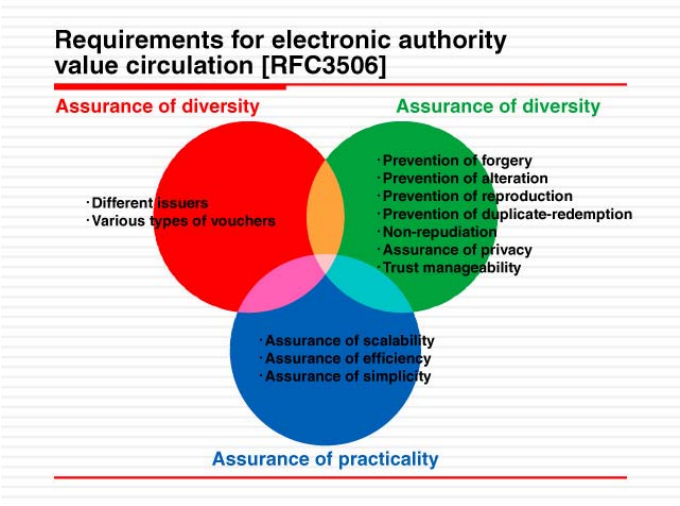

Figure 2 RFC requirements

The below explanation applies to the respective prerequisites indicated in Figure 2. Their descriptions appropriately supplement the explanation in RFC3506, while referring to [TKHF00].

Assurance of diversity

- Different issuers

  Unlike so-called electronic cash and electronic money, authority values can be generated by various core participants from individuals to companies and governments. These various core participants must be provided with the means for creating and issuing authority values.

- Various types of vouchers

  Though it is quite a task for an electronic cash and currency system just to handle the differences among the basic monetary units, electronic authority values must also deal with a multiplicity of other items, such as tickets and coupons.

Assurance of security

- Preventing forgery

  It must be assured that only the issuers will be able to create the authority values. That is to say, though the respective issuers (from among the different issuers) are stipulated for the authority values, there must be no arbitrary forging of authority values enabling others to become issuers.

- Preventing alteration.

  It must not be possible for the content of the authority values to be changed in the circulation process. Nonetheless it will be permissible for their owners to be changed through transfers. Only the owners (who are the transfer source) can be allowed to effect transfers of the authority values.

- Preventing reproduction

  The authority values must not be reproduced in the circulation process; in other words, a certain

authority value must only be possessed by one owner at most at certain time.

- Preventing duplicate-redemption
  Once it has been consumed, an authority value must not be useable thereafter. Moreover, it must be possible only for the owner to utilize the authority value.

- Non-repudiation
  The issuer must not be allowed to repudiate the issuance of the authority value. The owner must likewise be prevented from repudiating the transfer or consumption.

- Ensuring privacy
  The current or past owners of a certain authority value must be concealed from those who seek to acquire that authority value.

- Trust manageability
  If we assume an environment where various types of authority values circulate, it will be difficult for users to judge whether or not certain authority values can ‘trusted’ (whether or not they actually have value). This necessitates a function enabling them to judge whether an authority value can be trusted.

Assurance of practicality

- Scalability
  It must not be presumed that there will be volume brokers capable of single-handedly selling all authority values or authentication offices that will authenticate all issuers or owners. A system dependant on such a concentrated single office would be extremely fragile; a disruption in such an organization could lead to the failure of the entire system.

- Efficiency
  It must be possible to efficiently equip the system producing the authority values, to enable it to respond to high performance requirements, such as for event and transport tickets

- Simplicity
  The setup ((the standard specifications for the authority value circulation system) must be simple. Simplicity is important not only to reduce setup costs, but also for the understandability and credibility of the system itself.

The prerequisites drawn from the RFC3506 are required in order to securely issue and circulate the authority values as valuables possessing ‘value.’ Nonetheless, the actual circulation of authority values does not just entail simple one-way issuance and transfer, but rather is often done as a part of a ‘transaction,’ as discussed in “Usage scenarios” in section 2.1

Transaction fairness must be guaranteed to enable general consumers and merchants to conduct such transactions with confidence. In other words, from the user’s perspective it is necessary to prevent deprivation of the (authority values; money, product coupons, etc., as) price compensation, without receiving (authority values; entertainment tickets, etc. as) merchandise. Conversely, from the merchant’s perspective, it is necessary to prevent the transfer of the merchandise, without receiving the price compensation [THIF01]. These prerequisites are vital, particularly for transactions in a mobile environment where communication is prone to being intercepted.

Consequently, the following prerequisites are necessary to realize the secure authority value transactions discussed under “Usage scenarios” in section 2.1.

Assurance of fairness

The respective parties to the exchange must not lose the authority value to be transferred without receiving the authority value to be received as the consideration for the price. That is to say, the state when the exchange is finished must be such that either the authority value to be received or the authority value to be transferred is actually possessed. (assurance of fairness upon completion of the transaction). The exchange must always be concluded within the allotted time.

4. Outline of the TENeT specifications

4.1 TENeT characteristics

To enable the secure usage of authority values within various environments and in the mobile environment in particular, TENeT stores the authority values in tamper-proof devices, such as IC cards and USIMs. These are called TENeT IC cards. TENeT has adopted the "Optimistic Exchange Protocol for Fair Authority Value Transactions"[THIF01] technology to make possible the secure and fair circulation and transaction of authority values thorough networks. As a result, it possible to transact authority values, both securely and fairly, between IC cards located at a distance from each other, without inviting a concentrated on the server.

To facilitate the use of the above described exchange protocol type distributed processing between IC cards from application programs, TENeT has put together a mechanism for sending and receiving messages by dispersed type transmission between IC cards and between IC cards and application programs.

This adoption of these technologies has enabled TENeT to easily achieve various applications for confidently and securely circulating and transacting authority values in a mobile environment.

4.2 TENeT architecture

Figure 3 shows the various components comprising TENeT. Here following, we will we outline each of these components.

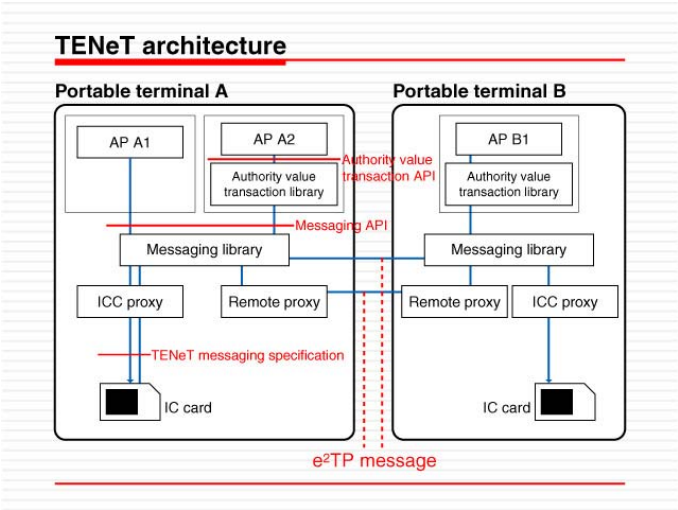

Figure 3TENeT architecture

4.3 Authority value circulation library

The authority value circulation library is a high level library for operating and transacting electronic authority values stored in TENeT IC cards. This library offers the functions provided by TENeT IC cards to application programs (AP). In other words, the developers of the general applications using TENeT specifications can use the API provided by this library alone to develop APs, without any awareness of the structure or specifications of the e^2TP messages delivered and received between the IC cards.

The TENeT specifications stipulate the authority value transaction API specifications as the API for using this library. The authority value transaction API specification is stipulated as a Java specification.

4.4 Messaging library

The messaging library is intended for sending and receiving e2TP (Extended eTP) messages, the communication messages used by TENeT, between IC cards and with other APs. e2TP messages are expanded eTP messages in the eTRON/ 16 specification.

The application can send and receive e2TP messages either synchronously (awaits blocks of response messages for transmitted messages) or asynchronously (continues processing without waiting for a response message, after sending a message). When an asynchronous message has been sent, the received message is supposed to be acquired by a listener registered in advance, simultaneously with the other event driven system (GUI framework, etc.).

An optional AP, IC card, server or the like with an eTRON ID in the TENeT name space can be specified as the e2TP message destination to be sent by this library. If the destination was remote, the message is automatically routed by this library and sent through the network to the appropriate destination. As a result, it is not necessary to be conscious of whether the destination is local or remote. However, when some messages are remotely sent to the IC card, they become invalid for security reasons. The types of messages that become invalid when sent remotely are defined by the TENeT IC card specification.

The eTRON ID of each AP in this library is created and acquired automatically using the IC card eTRON ID. This value is stored in the object that serves as the sending and receiving intermediary and is automatically allocated as the message transmission source ID when the message is sent. Consequently, the respective APs need not be aware of the specific eTRON ID assignments.

The TENeT specification stipulates the messaging API specification as the API for using this library. The messaging API specification is stipulated by Java.

4.5 TENeT IC card

IC cards play the role of storing and managing the authority values for TENeT. Users can use the TENeT IC card for such operations as transacting, creating and deleting authority values. TENeT IC cards have multiple ‘folders’ and the authority values created or received through transactions can be stored in any folder. TENeT IC cards also have a user authentication function that prevents accessing for improperly manipulating authority values.

Here following is a description of the functions provided by TENeT authority values.

Authentication function

• IC card authentication
  It authenticates that the user is an IC card owner.
• Folder/ file access control
  It sets the access privileges for folders and files.

Authority value management functions

• Folder creation and deletion
  Creates or deletes folders within a card or
• Folder list acquisition
  Acquires a list of folder information within a card
• Authority value creation
  Creates authority values in the specified folder within a card
• Authority value deletion
  Deletes the specified authority values within a card
• Acquisition of list of authority values (stored in the folder)
  Acquires all the authority value information located in a folder within a card.

Authority value circulation functions

• Transfer and exchange of authority values
  Transfers the specified authority values within a card or exchanges them with other authority values
• Release of interrupted transactions

When the above exchange and transfer processing has been interrupted, it releases the transactions and finishes their processing.

Operating system functions

• Backup and restoration of the content of an IC card

Externally backs up all the information within the card, such as when the folder size has been changed

Bibliography

[RFC3506] K. Fujimura, and D. Eastlake. RFC3506: Requirements and Design for Voucher Trading System (VTS), IETF, Mar. 2003.

[TKHF00] M. Terada, H. Kuno, M. Hanadate, and K. Fujimura. Copy Prevention Scheme for Rights Trading Infrastructure, In Proc. 4th Working Conference on Smart Card Research and Advanced Applications (CARDIS), pp. 51-70, IFIP, Sep. 2000.

[TKIF01] An Optimistic Fair Exchange Protocol for Trading Electronic Rights- Masayuki Terada (NTT DoCoMo, Japan), Makoto Iguchi, Masayuki Hanadate, Ko Fujimura (NTT, Japan) In Proc. 6th Working Conference on Smart Card Research and Advanced Applications (CARDIS), pp. 255-270, IFIP, Apr. 2004.