OSF DCE SIG
Request For Comments: 57.0

R. Merckling (HP)
A. Anderson (HP)

March 1994

SMART CARD INTRODUCTION

1. INTRODUCTION

Smart cards represent a new technology that has tremendous potential for enhancing the security of distributed systems. This RFC, 57.0, introduces smart card terminology, describes current smart card technology (including physical and logical characteristics), discusses the current status of smart card standardization, and closes with a brief discussion of the benefits DCE could gain by utilizing smart cards. A follow-on RFC, titled ‘‘DCE Smart Card Integration’’ [MER 57.1], describes a proposed DCE implementation.

2. TERMINOLOGY

(a) *Account*: A security database entry associating a principal with a key and other security-related information such as privileges.

(b) *Issuer*: In this RFC series, an organization that purchases smart cards and issues them to its users for use in accessing the issuer’s services or systems.

(c) *Dedicated file*: A smart card file containing file control information and, optionally, memory available for allocation. It may be the parent of elementary files and/or dedicated files [ISO 7816-4]; roughly, a smart card ‘‘file directory’’.

(d) *EEPROM*: Electrically Erasable Programmable Read-Only Memory.

(e) *Elementary file*: A set of data units or records in the smart card that share the same identifier [ISO 7816-4]; roughly, a smart card ‘‘file’’.

(f) *File control information (FCI)*: Logical, structural and security attributes of a file; a string of data bytes available in response to a SELECT FILE command [ISO 7816-4].

(g) *FRAM*: Ferro-Electric Random Access Memory.

(h) *GSM*: Groupe Special Mobile; European digital cellular telephone standard, providing security services such as user authentication, traffic confidentiality, and key distribution.

(i) *IC*: Integrated circuit. A single circuit containing multiple transistors.

(j) *Interactive principal*: A human user of a system. See ‘‘principal’’.

(k) *Key*: A parameter used in conjunction with a cryptographic algorithm that determines:

   (i) The transformation of plaintext data into ciphertext data,

   (ii) The transformation of ciphertext data into plaintext data,

   (iii) A digital signature, or

   (iv) A message authentication code [NIST 140].

(l) *Long-term key*: A key that is used over a relatively long period of time. Compare with ‘‘session key’’. In DCE, each principal has a unique long-term key that is used in authenticating a user or server claiming to be that principal. For interactive principals, the long-term DCE key is derived from the user’s password.

(m) *Master file*: The mandatory unique dedicated file representing the root of the smart card file structure [ISO 7816-4].

(n) *Message authentication code (MAC)*: A cryptographic checksum, based on DES [NIST 140].

(o) *Noninteractive principal*: A principal that is an instance of a DCE server, an instance of a DCE application server, a computer in a DCE cell, or a cell (more correctly, ''an Authentication Service surrogate''). See ''principal''.

(p) *Passivation layer*: A layer of dielectric material covering the circuitry on a smart card that protects the chip from impurities and dust and prevents passage of radiation associated with probes, such as electron-beam microscopy. Often referred to as a ''seal''.

(q) *Password*: A sequence of alphanumeric and punctuation characters entered by a user to authenticate to a computer system (including to a smart card).

(r) *PIN*: Personal Identification Number; a 4 to 12 character alphanumeric code or password used to authenticate a person's identity, commonly used in banking applications [NIST 140]. In connection with smart cards, this document uses the more general term ''password'' rather than ''PIN''.

(s) *Principal*: An entity that is capable of believing that it can communicate securely with another entity. In DCE Security, principals are represented as entries in the Registry database. See ''interactive principal'' and ''noninteractive principal'' [OSF 93].

(t) *Session key*: A random number generated to serve as a key for a specific transaction or set of transactions.

(u) *Smart card*: A credit card-sized, tamper-resistant security device that relies on VLSI chip technology for information storage and information processing.

(v) *User*: A person who attempts to access a computer system; a person who has been issued a smart card.

(w) *VLSI*: Very Large Scale Integration; integration of thousands or more transitors on a single chip, enabling single-chip implementations of CPU, RAM, ROM, etc.

3. SMART CARD TECHNOLOGY

3.1. Basic Concepts

A smart card is a credit card-sized, tamper-resistant security device that offers functions for secure information storage and information processing that rely on VLSI chip technology [GUIL 91]. A smart card actually contains a secure microprocessor chip embedded in the card. The chip can implement a secure file system, compute cryptographic functions, and actively detect invalid access attempts. With proper application of file system access rights, a smart card can be safely used by multiple, independent applications.

A smart card is distinguished from a magnetic stripe card (e.g., typical U.S. credit card) in that a magnetic stripe card has no VLSI circuitry, and thus no active security procedures and no built-in tamper-resistance. Anyone with an appropriate card reader can read whatever is on the card. The current cost for magnetic stripe cards (March 1994) is around $.50-$1.00 per card in quantities of 1000.

Smart cards are also distinguished from ''SuperSmart'' or ''token'' cards. These use a small LCD to display the time of day encrypted using an internal key that is programmed at the time of manufacture. Such cards have no storage capabilities and no interface to external computer systems. They perform a single, well-defined function that can be used in authentication protocols: users manually type the digits displayed on the card (which are updated periodically) as part of authenticating to a host. These cards are not capable of performing more extensive functions as part of a security system, and thus are not evolutionary. Cost (as of March 1994) for ''SuperSmart'' cards is on the order of $60/card in quantities of 250-500 (based on a cost of $20 per year, and battery lifetime of around 3 years).

3.2. Physical Characteristics

3.2.1. Card types

Within the family of smart cards, there are two general categories: cards with contacts and cards without contacts. Contact cards contain physical contact points on the surface of the card that allow transmission of commands, data, and status information between the card and a card reader. Contactless cards also require physical contact with a reader, but get their power via induction rather than through one of the contacts. This difference affects only the very lowest level (physical level) of the protocols used with smart cards.

3.2.2. Physical specifications

Focusing now on contact smart cards, potential uses depend on card specifications. Microprocessor and memory technology have steep technology curves, but the following specifications of typical available contact smart cards can serve as a current baseline (March 1994):

(a) Clock rate: 3.5-8 MHZ.

(b) Non-volatile memory: 8-16 Kbytes (for data storage).

(c) ROM: 8-16 Kbytes (for the card operating system).

(d) RAM: Around 256-500 bytes of RAM (for operating system computation).

(e) EEPROM: 2-8 Kbytes (externally-accessible, non-volatile).

(f) Write cycles: Approximately 10^4–10^5.

(g) Processing time: Average of about 60 milliseconds (including transmission time) to retrieve a 56-bit number from a protected elementary file on the card. Depends primarily on transmission time between the host system and the card reader, so varies depending on capacity of that line.

(h) Cost: On the order of $7-$12/card in quantities of 1000-5000; card reader cost is on the order of $150-200 each in quantities of 100-500.

In the next few years, 16-32 bit RISC processors running at 20MHZ are likely to become available on smart cards. This will define a new generation of smart cards, as the power requirements and frequency radiation of these processors can not be handled within the current [ISO 7816-1,2] standard format. By 1995, it is expected that FRAM technology will be available, supporting more write cycles (10^8). This technology may also be incorporated into the new generation, although currently it is too expensive. [SJB 93]

3.2.3. Physical security characteristics

Smart cards incorporate physical tamper-resistance circuitry that responds to tampering by inhibiting the output function. There is a dielectric ‘‘passivation layer’’ covering the chip. The passivation layer protects the chip from impurities and dust, and prevents passage of radiation associated with probes, including electron-beam microscopy. The circuitry is capable of reacting to light (indicating the passivation layer has been broken); temperature, voltage, and frequency fluctuations outside the specified operating range. There are physical memory protection mechanisms, including memory scrambling, which make reverse engineering more difficult and hinders an attack trying to erase a selected data item in memory. Fuses are used during the manufacturing cycle to permanently disable ‘‘test’’ mode(s) once tests have been passed and the card is ready for distribution to issuers.

Smart cards can be manufactured with varying levels of physical security features, with higher costs associated with higher levels of security. Purchasers must evaluate with the vendor the level of physical security appropriate to their application.

3.3. Logical Characteristics

The smart card processing unit executes a chip operating system that implements a hierarchical file system on the non-volatile memory of the card, and a set of access and control operations both for the card itself and for the file system.

The following descriptions of card data structures, card operations, and card security architecture are taken from [ISO 7816-4]. This document, although still a draft, is currently undergoing balloting through ISO. It is complete enough to indicate the general types of structures and operations that cards should be expected to support.

3.3.1. Data structures

The file system supports a special root directory file (‘‘master file’’), optional sub-directory files (‘‘dedicated files’’), and data files (‘‘elementary files’’). The identifiers of all files along the path from the master file down to a specific file unambiguously identify the specific file. All three categories of files contain control information, such as a file identifier, file name, specifications of record or data lengths in the file, etc.

The draft standards specify various types of elementary file structures: a sequence of records of identical length, a sequence of records of variable length, a sequence of records with identical length organized as a ring, and a ''transparent structure'' that is seen at the interface as a sequence of data units.

3.3.2. Operations

The following commands are a subset of those specified in [ISO 7816-4], and are included here merely to give a basic understanding of the types of operations supported on smart cards.

(a) READ BINARY — Return all or part of the contents of an elementary file.

(b) WRITE BINARY — Write binary values into an elementary file.

(c) ERASE BINARY — Erase all or part of the contents an elementary file.

(d) SELECT FILE — Set a ''current file'' that may be referred to implicitly in subsequent commands.

(e) VERIFY — Compare verification data sent from the host system with reference data stored in the card (e.g., a password).

(f) INTERNAL AUTHENTICATE — Compute authentication data using challenge data sent from the host system and a relevant secret (e.g., a key) stored in the card.

(g) EXTERNAL AUTHENTICATE — Conditionally update the security status of the card based on the result of a computation based on a challenge previously issued by the card, a key stored in the card, and authentication data sent from the host system.

3.3.3. Security architecture

Smart cards implement three levels of logical access control. The first is the association of a set of privileges with a user's password, and the ability to control access to files on the card based on those privileges. The second level of logical access control is the ability to detect and respond to a sequence of invalid access attempts. The third level is the ''logical channel'' — a logical link between the host system and a file on the smart card.

3.3.3.1. Privileges and access control

Two categories of access control mechanisms are promoted today in the smart card market. Both mechanisms are built-in characteristics of the relation between privileges and users for given objects.

(a) One system is the combinational system, where privileges are a first order logic function between authorization variables (v[i]). For example f(v[1], v[2], ..., v[n], p1) will be TRUE for a user/subject for a READ access, if and only if the user/subject knows the values of every authorization variable v[i] AND knows the password p1. The function f is combinational, e.g., (v[1] AND v[2] OR v[3] XOR v[4]) AND value_in_pwd_filex_of(p1).

(b) The second system is a sequential system where privileges are the result of a sequential function between authorization variables (v[i]). For example, f(v[1], v[2], ..., v[n], p1) gives READ access for an object to a user/subject, if and only if the user/subject knows which values (v[i]) have to be presented in state s[k], where k identifies a sequential file selection and key presentation step. s[k] is determined by the current selected file and the current keys activated.

3.3.3.2. Invalid access attempts

Most, but not all, smart cards keep a record of sequential invalid access attempts (a supplied set of parameters for a function that fail to evaluate to TRUE), and deny further access to the card (or to the targetted file) once the count reaches a certain limit. In some cards the limit is configurable, while in others it is fixed at a small number such as 3 or 7. The count is reset to 0 when a valid access is made. Exceeding the limit either invalidates the card entirely, or puts it in a state where only a limited set of operations is available. These limited operations may be sufficient for an administrator to restore access.

Denial of access after a small number of invalid attempts prevents ''password guessing'' attacks on the card.

3.3.3.3. Logical channels

A ‘‘logical channel’’ is a logical link between the host system and a file on the smart card, either the Master File, a Dedicated File, or an Elementary File. When logical channels are in use, the selection of a file associates the file and its security status with the logical channel encoded in a reserved field of the selection command header.

Logical channels provide a mechanism for allowing multiple, independent applications to use the storage capabilities of the card. The card interface software on the host system must manage the mapping between processes and logical channels; the channel numbers are either assigned by the external world or by the card itself.

The logical channel portion of [ISO 7816-4] conveys 2 concepts. The first one deals with a logical link to files and requires the outside world to manage the channel numbers. In the second concept, the card allocates the logical channel number and supports a mechanism similar to swapping with a stack number. In both situations, cards implementing these standards grant applications the same control of access to files and data structures (without losing the security status) as if only one application had access.

3.4. Life Cycle

As stand-alone active entities, smart cards have a life-cycle and actors.

First, some terminology. The ‘‘chip manufacturer’’ is responsible for the chip design, production, and testing. The ‘‘card manufacturer’’ embeds the chip into the plastic card. The ‘‘card issuer’’ creates, designs, and prints the end-user organization’s logo onto the plastic card. The ‘‘card holder’’ is the user whose name is printed on the outside of the card at the same time it is written to a file inside the card file system.

The following life-cycle is typical for single-application smart cards:

- (a) Internal architecture development.
  - (i) Control structure(behavioral) development customization.
  - (ii) Data structure development.
- (b) Plastic card manufacturing.
- (c) Chip production and testing.
- (d) Smart card manufacturing.
- (e) Smart card preparation.
  - (i) Control structure(behavioral) customization.
  - (ii) Data structure customization.
- (f) Application preparation.
- (g) Use.
- (h) Invalidation.

The internal architecture development stage is used to develop the control and data structures that is best suited to the requirements of applications that will use the card. Some structures might not be architected, and might be left open to future application developments and extensions. Once an architected solution is found, it defines a permanent configuration specifying the file directory structure, and card behavior: it becomes a solution model. This solution model is a solution for a given problem (for example, a GSM solution model or a DCE solution model) that can be reproduced and manufactured. Multiple card manufacturers can reproduce the solution model if the solution specification follows interoperability characteristics.

The next requirement is for the chip for a card to be manufactured and given a unique serial number that identifies characteristics of manufacture (IC lot number, wafer number, die number, test equipment numbers, etc.). The chip then undergoes a self-test process that results either in an invalid, erased chip, or a valid chip with no non-user modes enabled. After this stage, there is no access to card memory addresses except under the control of the card operating system. Tamper-resistance circuitry has been activated.

Independent of chip manufacture, plastic card manufacture occurs.

During the smart card manufacturing stage, a chip is embedded into the plastic card. The card can be printed with the issuer's logo at this point or later.

The smart card preparation stage creates the externally-downloadable control structure and downloads it to the smart card — changing the basic behavior of the smart card, specifying the file structure that will exist on the card, associating rights, keys, and privileges with directories and files through various primitive card access and control operations (see Card Security Architecture), as well as setting basic card control parameters such as number of allowed invalid access attempts.

If the smart card preparation stage is not integrated with the application preparation stage, cards need to be transported from the card manufacturer to the end-user. In this case, the keys written at the smart card preparation stage are termed ''transport keys'' or ''initialization keys''. These keys are sent to the card issuer by the manufacturer separately from the cards. They prevent modification of the cards during transport from the manufacturer to the issuer. Once in possession of the transport keys, the issuer can access the card to perform the application preparation stage.

For security purposes, the card manufcaturer can permanently set rights and privileges before cards can move to the application preparation stage.

The application preparation stage initializes the card password(s), the data in the card file system, and optionally writes the user's name on the card. Some cards accept dynamic update, creation and deletion of files in the file structure after the application preparation stage (depending on the card preparation stage), but others enforce a fixed file structure once application preparation has taken place.

Then follows a stage of active card usage, during which the operations defined in the card preparation stage may be performed using the passwords defined during the card preparation stage. Usually, passwords and keys may be changed during the usage stage.

During the final stage of the card lifecycle, the card is invalidated. Cards should not be re-used in order to avoid any problems in organizational policy that might arise from having two users associated over time with the same card serial number. Invalidation of multi-application cards can be complex if internal applications are tied to the exterior appearance of the card: if one application is invalidated, then the issuer logo on the card may be confusing for the user. If the entire card must be invalidated in order to invalidate one expired application, then the user must obtain a new card in order to maintain access to the remaining applications.

4. STANDARDS

See [GUIL 91] for an excellent discussion of the international status of smart card standardization which is still fairly current.

Several parallel, overlapping ISO standardization efforts exist:

(a) ISO/IEC JTC1/SC17/WG4 (Information Systems — Identification Cards — Integrated Circuit Cards with Contacts) has produced specifications of the physical characteristics [ISO 7816-1,2] and physical communication protocols [ISO 7816-3] that are International Standards. The specification of the file system layer [ISO 7816-4] is still a Committee Draft, but is currently undergoing balloting. Other standards are still in Working Draft stage.

The following standards apply for ISO SC17/WG4 contact cards:

```
Standard          Scope
-----------       ----------------------------------
   7816-6         Common Data Elements (unpublished)
IS 7816-5         Registration for Applications
CD 7816-4.2       Commands for Interchange
IS 7816-3         Transmission Protocol
IS 7816-2         Contact Location
IS 7816-1         Physical Characteristics
```

As long as the lower layers conform to [ISO 7816-4] and the transmission protocol is T=0 (asynchronous, half-duplex character transmission protocol) or T=1 (asynchronous, half-duplex block transmission protocol), the link between the card reader and the host system can be implemented via RS232, PCMCIA, Infra-Red, etc.

(b) ISO TC68/SC6 (Banking — Financial Transaction Cards, Related Media and Operations) has two working groups: WG5 (Messages Exchanged with Integrated Circuit Cards) has produced a Draft International Standard and a Working Draft [ISO 9992] dealing with messages and data elements. WG7 (Security Architecture of Banking Systems Using Integrated Circuit Cards) has produced a Draft International Standard and a Working Draft covering card life cycle, keys, and algorithms.

(c) ISO/IEC JTC1/SC17/WG8 (Information Systems — Identification Cards — Contactless Integrated Circuit Cards) has not produced standards to date in the [ISO 10536] series.

(d) Specific ANSI X3B10.x groups cover contactless cards. The ANSI X3B10.1 group covers IC cards with contacts. ANSI is circulating a slightly modified version of [ISO 7816-3].

(e) The FIPS on Security Requirements for Cryptographic Modules [NIST 140], which is in draft status, specifies general physical, functional, and process requirements for four increasing levels of security, but does not specify interfaces or protocols. This standard applies to government applications using cryptographic functions of smart cards.

(f) There are a few other standards bodies that have developed smart card standards for specific industry segments or applications. See [GUIL 91] for a discussion of these.

Due to the state of standardization, it is not possible to specify a standard interface to smart cards or smart card devices except at the physical layer. The draft for the file system layer, however, at least provides us with a general picture. Based on this, it is possible to specify an abstract usage model and high-level interface that should be implementable with minimal software ‘‘glue’’ using cards from most vendors.

5. WHY SMART CARDS IN DCE?

We have now seen the functions smart cards are capable of performing. What value do these present for DCE in particular?

There are three basic potential areas of value: two-factor authentication, secure storage, and encryption and key generation.

5.1. Two-Factor Authentication

Without smart cards, DCE uses one-factor authentication: users authenticate by proving they know a secret that is shared with the DCE Security Service, i.e., the user’s password. Passwords are known not to be very secure, as they can be lost, stolen, shared, or guessed fairly easily [HAGA 91, HARR 76].

By using smart cards to store each user’s long-term DCE key, the cards introduce a second authentication factor: users now must not only prove they know a secret (the password used to gain access to the card), but they must also prove they have physical possession of the smart card (by using the password and successfully retrieving the long-term key).

The use of two-factor authentication dramatically improves security. Cards limit vulnerability to sharing, since the card can be in the physical possession of only one individual at a time. They also effectively prevent vulnerability to guessing, since the long-term key stored on the card is a 56-bit random number rather than a password. Cards can be lost or stolen, but without the accompanying card-access password, they are not usable. Should the card be lost or stolen, the owner is highly motivated to report the loss promptly, as the owner will be unable to access the computer system without the card.

5.2. Secure Storage

The second potential value that smart cards present to DCE is their secure storage capability. This is utilized in two-factor authentication for storing a user’s long-term key. It would also be feasible to decrypt and store DCE credentials on the card, hiding them from the host system and from attackers on the host. DCE applications could also make use of secure storage on the card for application-specific information.

5.3. Encryption and Key Generation

The third potential value to DCE is the encryption and key generation capabilities that smart cards have. Licensing agreements for public key technology are typically much less restrictive when the technology is confined to a physical device. By storing the user's private keys in secure card storage, and using card encryption capabilities to generate authentication information from the keys, the encryption technology need not be implemented in the host system. The cards' ability to generate random numbers may also be useful as a source for keys.

6. ACKNOWLEDGMENTS

The following members of the HP Chelmsford System Software Lab were significant contributors to this RFC: Maryann Hondo, Sean Mullan, and Joe Pato.

Gilles Lisimaque reviewed an early draft, providing extensive helpful comments and corrections. Mr. Lisimaque is a member of ISO/IEC JTC1/SC17/WG4, a member of ANSI X3B10.1, and is cochairman of the Technical Committee of the Smart Card Forum. Mr. Lisimaque is one of the founders of Gemplus Card International and Executive Vice President of Gemplus Card International Corp, Gaithersburg, MD.

REFERENCES

[GUIL 91] Louis Claude Guillou, Michel Ugon, and Jean-Jacques Quisquater, ''The Smart Card — A Standardized Security Device Dedicated to Public Cryptology'', in Gustavus Simmons, ''Contemporary Cryptology — The Science of Information Integrity'', IEEE Press, pp.561-614, 1992.

[HAGA 91] W. J Haga and M. Zviran, ''The Practice of Passwords Usage: Some empirical Evidence'', p164-172, 7th Int. Conference on Information Security, Brighton, May 1991.

[HARR 76] M Harrison and W. L Ruzzo, ''Protection in Operating Systems'', Comm of the ACM. Aug 76 Vol 19 Number 8 p 470–-491.

[KOHL 93] J. Kohl and C. Neumann, ''The Kerberos Network Authentication Service'', Internet Entgineering Task Force, Networking Group, Internet Draft RFC 1510, Sep 1993.

[KRAJ 93] Marjan Krajewski, Jr., "Smart Card Augmentation of Kerberos", Proceedings of the Privacy and Security Research Group Workshop on Network and Distributed System Security, February 11-12, 1993, San Diego, CA, pp.119-123.

[MUFT 89] Sead Muftic, ''Security Mechanisms for Computer Networks'', 1989.

[ISO 7816-1] ISO, ''IS 7816-1: Identification cards — Integrated circuit(s) cards with contacts — Part 1: Physical Characteristics'', 1987.

[ISO 7816-2] ISO, ''IS 7816-2: Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and Locations of Contacts'', 1988.

[ISO 7816-3] ISO/IEC, ''IS 7816-3: Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocols'', 1989.

[ISO 7816-3.1] ISO/IEC, ''IS 7816-3, Amendment 1: 1989, Identification cards — Integrated circuit(s) cards with contacts — Clause 9 to be inserted in part 3: Protocol type T=1, asynchronous half duplex block transmission protocol'', December 1992.

[ISO 7816-3.2] ISO/IEC, ''7816-3, Amendment 2: 1994, Identification cards — Integrated circuit(s) cards with contacts — Revision of protocol type selection''. Not published.

[ISO 7816-4] ISO/IEC, ''CD 7816-4.2: Information Technology — Identification Cards. Integrated Circuit(s) Cards with Contacts, Part 4, Inter-industry commands for Interchange'', CD ballot 7186-4.2 circulated for vote by SC17 on 12/14/93. Also available for ANSI members under the reference X3B10 94/562.

[ISO 7816-5] ISO/IEC, ''IS 7816-5: 1992, Identification cards — Integrated Circuit(s) Cards with Contacts — Part 5: Numbering System and Registration Procedure for Application Identifiers, by ISO/IEC JTC 1/MW4/WG4, 9/24/92.

[ISO 7816-6] ISO/IEC, ‘‘7816-6: 199x, Identification cards — Integrated circuit(s) cards with contacts — Part 6: Inter-industry data elements’’, by ISO/IEC JTC 1/SC 17/WG 4 N1016. Not published.

[ISO 9992-1] ISO, ‘‘DIS 9992-1: Financial Transaction Cards — Messages between the integrated circuit card and the card accepting device — Part 1: Concepts and Structures’’, by TC68/SC6/WG5.

[ISO 9992-2] ISO, ‘‘WD 9992-2: Financial Transaction Cards — Messages between the integrated circuit card and the card accepting device — Part 2: Functions, messages (commands and responses), data elements and structures’’, by TC68/SC6/WG5.

[ISO 10202-1] ISO, ‘‘DIS 10202-1: Financial Transaction Cards — Security Architectures of Banking Systems Using Integrated Circuit Cards — Part 1’’, by TC68/SC6/WG7.

[ISO 10202-x] ISO, ‘‘WD 10202-x: Financial Transaction Cards — Security Architectures of Banking Systems Using Integrated Circuit Cards — Part X’’, by TC68/SC6/WG7.

[ISO 10536] ISO, ‘‘10536: Information Systems — Identification Cards — Contactless Integrated Circuit Cards’’, by ISO/IEC JTC1/SC17/WG8. Not published.

[MER 57.1] Roger Merckling and Anne Anderson, ‘‘OSF/DCE SIG RFC 57.1: DCE Smart Card Integration’’, March 1994.

[NIST 140] NIST, ‘‘FIPS DRAFT 140-1 — Security Requirements for Cryptographic Modules’’, April 1991.

[OSF 93] OSF, ‘‘OSF DCE Application Development Guide — Part 6. DCE Security Service — Chap 40. Authentication’’, Revision 1.0, Prentice Hall, Dec 1993.

[PATO 93] Joe Pato, ‘‘OSF/DCE SIG RFC 26.0: Use of pre-authentication to avoid password guessing attacks’’, June 1993.

[SJB 93] ‘‘Smart card chip trends and development’’, in Card & Technology Today, April 1993, Sarah J Brown edition, pp. 12-14

AUTHORS’ ADDRESSES

Roger Merckling
Hewlett-Packard France
38053 Grenoble Cedex 9
Etablissement de Grenoble
5, avenue Raymond Chanas
38320 EYBENS
France

Internet email: Roger_Merckling@hp6300.desk.hp.com
Telephone: 33-76-62-1131

Anne Anderson
Hewlett-Packard Company
300 Apollo Drive
Chelmsford, MA 01824
USA

Internet email: aha@ch.hp.com
Telephone: 1-508-436-5707