TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 8461-2:2010
ISO 9564-2:2005

Xuất bản lần 1

NGÂN HÀNG – QUẢN LÝ BẢO MẬT SỐ NHẬN DẠNG CÁ NHÂN – PHẦN 2: PHÊ CHUẨN THUẬT TOÁN MÃ HOÁ PIN

Banking – Personal Identification Number management and security - Part 2: Approved algorithms for PIN encipherment

HÀ NỘI - 2010

Lời nói đầu

TCVN 8461-2:2010 hoàn toàn tương đương với ISO 9564-2:2002.

TCVN 8461-2:2010 do Ban kỹ thuật Tiêu chuẩn quốc gia TCVN/TC 68 "*Tài chính ngân hàng và tiền tệ*" biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ công bố.

Bộ TCVN 8461 (ISO 9564) *Ngân hàng- Quản lý bảo mật số nhận dạng cá nhân* gồm 2 phần:

- TCVN 8461-1 (ISO 9564-1) - Phần 1: Nguyên tắc cơ bản và yêu cầu đối với trao đổi PIN tại các hệ thống rút tiền.

- TCVN 8461-2 (ISO 9564-2) - Phần 2: Phê chuẩn thuật toán mã hoá PIN.

Bộ (ISO 9564) *Banking – Personal Identification Number management and security* còn có các phần:

- Part 3: Requirements for offline PIN handling in ATM and POS systems.

- Part 4: Guidelines for PIN handling in open networrks.

Ngân hàng – Quản lý bảo mật số nhận dạng cá nhân – Phần 2: Phê chuẩn thuật toán mã hoá PIN

Banking – Personal Identification Number management and security -
Part 2: Approved algorithms for PIN encipherment

1 Phạm vi áp dụng

Tiêu chuẩn này qui định việc mã hóa bằng thuật toán đối với số nhận dạng cá nhân (PINs). Những thuật toán này bao gồm thuật toán mã hóa dữ liệu (DEA) và thuật toán mã hóa RSA theo những quá trình thiết lập thuật toán cơ bản qui định trong TCVN 8461-1 (ISO 9564-1).

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây là rất cần thiết cho việc áp dụng tiêu chuẩn. Đối với tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các bản sửa đổi.

TCVN 8461-1 (ISO 9564-1), Ngân hàng – Quản lý bảo mật số nhận dạng tài khoản cá nhân – Phần 1: Nguyên tắc cơ bản và yêu cầu đối với trao đổi số PIN tại các hệ thống rút tiền.

ISO 9564-3, Banking – Personal Identification Number management and security - Part 3: Requirements for offline PIN handling in ASTM and POS systems. (*Ngân hàng – Quản lý bảo mật số nhận dạng tài khoản cá nhân – Phần 3: Yêu cầu về đối với trao đổi PIN ngoại tuyếntại các hệ thống rút tiền tự động).*

ISO/IEC 10116, Information technology – security techniques – modes of operation for an n-bit block cipher (*Công nghệ thông tin - Kỹ thuật bảo mật – Phương thức vận hành đối với mật mã khối n-bit).*

ISO 11568-2, Banking – key management (retail) – Part 2: key management techniques for symmertric (*Ngân hàng – Quản lý mã khóa (lĩnh vực bán lẻ)- Phần 2: Kỹ thuật quản lý mã khóa sử dụng mật mã đối xứng*).

EMV 2000, Integrated Circuit Card Specification for Payment Systems Book 2: Security and Key Management (*Tiêu chuẩn thẻ Chíp cho các hệ thống thanh toán, Quyển 2: Bảo mật và quản lý mã khóa*).[1)]

ANSI INCITS 92-1981, Data Encryption Algorithm [formerly ANSI X3.92-1981 (R1998)] (*Thuật toán mã hóa dữ liệu [trước đây là Chuẩn ANSI X3.92-1981 (R1998)]*.[2)]

ANSI X9.52-1998, Triple Data Encryption Algorithm Modes of (*Phương thức vận hành thuật toán mã hóa dữ liệu ba lần).*

AS 2805.5.3-1992, Electronic funds tranfer – Requirement for interfaces – Ciphers- Data encipherment algorithm 2 (DEA2) (*Chuyển tiền điện tử - Quy định về giao diện – Mật mã - Thuật toán mã hóa dữ liệu 2 (DEA 2).*[3)]

3 Mã hóa dữ liệu (DEA)

3.1 Định nghĩa

Việc định nghĩa DEA phải phù hợp với ANSI X3.92:1981.

3.2 Yêu cầu kỹ thuật

Mã hóa các khối PIN sử dụng thuật toán TDEA phù hợp TCVN 8461-1 (ISO 9564-1) phải được thực hiện bằng cách sử dụng thuật toán theo chế độ Bảng tra mã điện tử (ECB) (với độ dài khối n=64) theo ISO/IEC 10116. Mỗi thao tác mã hóa/ giải mã theo thuật toán TDEA là một thao tác kết hợp của các thao tác mã hóa/ giải mã theo thuật toán DEA được định nghĩa trong ISO 11568-2 và ANS X9.52.

4 Thuật toán RSA

4.1 Định nghĩa

Định nghĩa thuật toán RSA[4)] phải phù hợp với định nghĩa trong AS 2805.5.3:1992.

4.2 Yêu cầu kỹ thuật

Mã hóa các khối PIN sử dụng thuật toán RSA theo ISO 9564-3 phải phù hợp với chuẩn EMV 2000, Quyển 2.

4.3 Khả năng áp dụng

Chỉ sử dụng thuật toán được phê chuẩn này trong ISO 9564-3.

---

1) EMV: chuẩn EMV do các tổ chức thẻ Europay, MasterCard, VISA xây dựng

2) Viện tiêu chuẩn quốc gia Hoa kỳ.

3) Viện tiêu chuẩn Úc.

4) Tên nhà sáng chế Ronald Rivest, Adi Shamir và Leonard Adleman.