TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 7818-2 : 2007

ISO/IEC 18014-2 : 2002

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN - KỸ THUẬT MẬT MÃ DỊCH VỤ TEM THỜI GIAN PHẦN 2: CƠ CHẾ TOKEN ĐỘC LẬP

Information technology – Cryptographic technique – Stamping services

Part 2: Mechanisms producing independent tokens

HÀ NỘI – 2007

Mục lục

Trang

Lời nói đầu

TCVN 7818-2 : 2007 hoàn toàn tương đương với ISO/IEC **18014-2 : 2002**

TCVN 7818–2 : 2007, Tiểu ban Kỹ thuật Tiêu chuẩnTCVN/JTC1/SC27 "*Các kỹ thuật mật mã*" biên soạn, Ban Cơ yếu Chính phủ đề nghị, Bộ Khoa học và Công nghệ công bố.

Xuất bản lần 1

Công nghệ thông tin – Kỹ thuật mật mã – Dịch vụ tem thời gian Phần 2: Dịch vụ Token độc lập

Information technology – Cryptographic techniques – Time – Stamping services
Phần 2: Mechanisms producing independent tokens

1 Phạm vi áp dụng

Dịch vụ tem thời gian cung cấp bằng chứng về sự tồn tại của một mục dữ liệu trước một thời điểm xác định theo thời gian. Các dịch vụ tem thời gian tạo ra các thẻ tem thời gian, đó là một cấu trúc dữ liệu chứa một sự gắn kết có thể kiểm tra được về mặt mật mã giữa sự trình bày một mục dữ liệu và một giá trị thời gian. Tiêu chuẩn này trình bày các cơ chế tạo tem thời gian độc lập, các thẻ tem thời gian này có thể được kiểm tra một cách riêng biệt.

2 Tài liệu viện dẫn

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

ISO 7498-2:1989, Information processing systems – Open Systems Interconnection – Basic reference Model – Part 2: Secirity Architecture (Các hệ thống xử lý thông tin - Liên kết các Hệ thống mở - Kiểu tham chiếu cơ bản - Phần 2: Kiến trúc an toàn).

ISO/IEC 8824-1: 1998 | ITU-T Recommendation X.680 (1997), Information technology – Abstract Systax Notation One (ASN.1): Specification of basic notation (Bản công bố X.680 (1997), Công nghệ thông tin – Cú pháp tóm lược Ký hiệu dạng một (ANS.1): Quy định ký hiệu cơ sở).

ISO/IEC 8824-2: 1998 | ITU-T Recommendation X.681 (1997), Information technology – Abstract Systax Notation One (ASN.1): Information object specification (Bản công bố X.681 (1997), Công nghệ thông tin – Cú pháp tóm lược Ký hiệu dạng 1 (ANS.1): Quy định đối tượng thông tin).

ISO/IEC 8824-3: 1998 | ITU-T Recommendation X.682 (1997), Information technology – Abstract Systax Notation One (ASN.1): Constraint specification (Bản công bố X.682 (1997), Công nghệ thông tin – Cú pháp tóm lược Ký hiệu dạng một (ANS.1): Quy định ràng buộc).

ISO/IEC 8824-4: 1998 | ITU-T Recommendation X.683 (1997), Information technology – Abstract Systax Notation One (ASN.1): Parameterisation of ASN.1 specifications (Bản công bố X.683 (1997), Công nghệ thông tin – Cú pháp tóm lược Ký hiệu dạng một (ANS.1): Quy định tham số ASN.1).

ISO/IEC 8825-1:1998 | ITU-T Recommendation X.690 (1997), Information technology – ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and