TCVN 13175:2020

ISO/IEC 29150:2011

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - KÝ MÃ

Information technology - Security techniques - Signcryption

HÀ NỘI - 2020

Mục Lục

Lời nói đầu

TCVN 13175 : 2020 hoàn toàn tương đương với ISO/IEC 29150:2011 và đính chính kỹ thuật 1:2011.

TCVN 13175 : 2020 (ISO/IEC 29150:2011) do Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã biên soạn, Ban Cơ yếu Chính phủ đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Công nghệ thông tin – Các kỹ thuật an toàn – Ký mã

Information technology – Security techniques – Signcryption

1 Phạm vi áp dụng

Tiêu chuẩn này quy định bốn cơ chế ký-mã có sử dụng các kỹ thuật mã hóa khóa công khai trong đó yêu cầu cả người khởi tạo và người nhận dữ liệu được bảo vệ phải có cặp khóa công khai và khóa riêng.

Tiêu chuẩn này không áp dụng cho các cơ sở hạ tầng để quản lý các khóa công khai được định nghĩa trong TCVN 7817-1 (ISO/IEC 11770-1) và ISO/IEC 9594.

CHÚ THÍCH 1 Các cơ chế ký-mã được xác định các cách xử lý xâu dữ liệu với các mục tiêu an toàn sau:

- **Bí mật dữ liệu**, tức là bảo vệ chống tiết lộ dữ liệu trái phép;
- **Toàn vẹn dữ liệu**, tức là việc bảo vệ mà cho phép người nhận dữ liệu xác minh rằng nó chưa được sửa đổi;
- **Xác thực nguồn gốc dữ liệu**, tức là việc bảo vệ mà cho phép người nhận dữ liệu xác minh danh tính của người khởi tạo dữ liệu;
- **Không thể giả mạo dữ liệu**, tức là việc bảo vệ chống lại việc sửa đổi dữ liệu trái phép, ngay cả bởi người nhận dữ liệu.

Bốn mục tiêu an toàn này không nhất thiết phải loại trừ lẫn nhau. Mục tiêu thứ tư, không thể giả mạo dữ liệu, là một khái niệm an toàn mạnh hơn mà bao hàm cả tính toàn vẹn dữ liệu và xác thực nguồn gốc dữ liệu.

CHÚ THÍCH 2 Hai trong số các cơ chế được quy định trong tiêu chuẩn này, cơ chế DLSC và ECDLSC, yêu cầu sử dụng các tham số khóa công khai trên toàn hệ thống cho cả người gửi và người nhận dữ liệu. Trong một hệ thống tồn tại nhiều cặp người gửi và người nhận, các tham số hệ thống giống nhau được yêu cầu sử dụng cho tất cả những người dùng này. Hai cơ chế còn lại là IFSC và EtS không yêu cầu sử dụng các tham số khóa công khai trên toàn hệ thống như vậy.

CHÚ THÍCH 3 Khi chọn bốn cơ chế ký-mã từ rất nhiều kỹ thuật đã được công bố và sử dụng để đưa vào tiêu chuẩn này, bảy tiêu chí tương tự như phụ lục A, trong ISO/IEC 18033-1:2005, cũng được áp dụng trong tiêu chuẩn này. Việc loại trừ các phương thức cụ thể không có nghĩa là các phượng thức đó không an toàn.

CHÚ THÍCH 4 Tiêu chuẩn này có sự tương đồng về mặt khái niệm với TCVN 12197 (ISO/IEC 19772) [14] trong đó quy định một số cơ chế mã hóa có xác thực, nghĩa là cơ chế đồng thời đảm bảo được tính toàn vẹn và bí mật của thông điệp. Sự khác biệt chính giữa TCVN 12197 (ISO/IEC 19772) và Tiêu chuẩn này là (1) các cơ chế được quy định trong TCVN 12197 (ISO/IEC 19772) thuộc danh mục kỹ thuật mật mã đối xứng, trong khi các cơ chế được quy định trong Tiêu chuẩn này là đại diện của kỹ thuật mật mã phi đối xứng; (2) trong khi tất cả các cơ chế được định nghĩa trong TCVN 12197 (ISO/IEC 19772) và Tiêu chuẩn này đảm bảo tính toàn vẹn và xác thực nguồn gốc dữ liệu, thì các cơ chế được định nghĩa Tiêu chuẩn này còn đảm bảo tính không thể giả mạo dữ liệu, ngay cả bởi người nhận dữ liệu.

2 Tài liệu viện dẫn

Các tài liệu sau đây, toàn bộ hoặc một phần, được dùng để tham chiếu trong tiêu chuẩn này và là không thể thiếu được đối với ứng dụng của nó. Đối với các tài liệu viên dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

TCVN 12855-2 (ISO/IEC 9796-2:2010), Công nghệ thông tin - Các kỹ thuật an toàn - Chữ ký số cho khôi phục thông điệp - Phần 2: Các cơ chế dựa trên phân tích số nguyên.

TCVN 12214-1 (ISO/IEC 14888-1:2008), Công nghệ thông tin - Các kỹ thuật an toàn - Chữ ký số kèm phụ lục - Phần 1: Tổng quan