TCVN TIÊU CHUẨN QUỐC GIA

TCVN 13178-1 : 2020
ISO/IEC 20009-1 : 2013
Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – XÁC THỰC THỰC THỂ ẨN DANH PHẦN 1: TỔNG QUAN

Information technology – Security techniques – Anonymous entity authentication – Part 1: General

HÀ NỘI – 2020

Mục lục

Lời nói đầu

TCVN 13178-1 :2020 hoàn toàn tương đương với ISO/IEC 20009-1:2013.

TCVN 13178-1 :2020 (ISO/IEC 20009-1:2013) 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.

Bộ tiêu chuẩn TCVN 13178 *Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể ẩn danh* gồm các tiêu chuẩn sau:

- TCVN 13178-1:2020 (ISO/IEC 20009-1:2013) Công nghệ thông tin các kỹ thuật an toàn - Xác thực thực thể ẩn danh - Phần 1: Tổng quan.

- TCVN 13178-2:2020 (ISO/IEC 20009-2:2013) Công nghệ thông tin các kỹ thuật an toàn - Xác thực thực thể ẩn danh - Phần 2: Các cơ chế dựa trên chữ ký số sử dụng một nhóm khóa công khai.

- TCVN 13178-4:2020 (ISO/IEC 20009-4:2017) Công nghệ thông tin các kỹ thuật an toàn - Xác thực thực thể ẩn danh - Phần 4: Các cơ chế dựa trên bí mật yếu.

Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể ẩn danh–

Phần 1: Tổng quan

Information technology – Security techniques – Anonymous entity authentication – Part 1: General

1 Phạm vi áp dụng

Tiêu chuẩn này quy định mô hình, các yêu cầu và ràng buộc đối với các cơ chế xác thực thực thể ẩn danh cho phép một thực thể được xác thực một cách hợp lệ.

2 Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa dưới đây.

2.1

Độ mạnh ẩn danh (anonymity strength)

Con số được xác định bằng xác suất mà một thực thể trái phép có thể xác định chính xác người ký tên thực sự từ một chữ ký đã cho

CHÚ THÍCH 1 Giá trị của độ mạnh ẩn danh bằng *n* có nghĩa là xác suất mà một thực thể trái phép có thể đoán chính xác người ký tên thực sự từ một chữ ký là 1/*n*.

[NGUỒN: ISO/IEC 20008-1]

2.2

Xác thực thực thể ẩn danh (anonymous entity authentication)

Sự chứng thực rằng một thực thể sở hữu các thuộc tính nhất định, mà không phân biệt thực thể này với các thực thể khác có cùng các thuộc tính đó

2.3

Chữ ký số ẩn danh (anonymous digital signature)