TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 8066: 2009

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – KHUÔN DẠNG CHỨNG THƯ SỐ

Information technology – Digital certificate format

HÀ NỘI – 2009

Mục lục

Lời nói đầu

TCVN 8066:2009 được xây dựng trên cơ sở chấp nhận áp dụng Khuyến nghị X.509 (8/2005) của Liên minh Viễn thông Thế giới (ITU-T); tài liệu RFC 3280 (4/2002) và RFC 3281 (4/2002) của Nhóm đặc trách về Internet (IETF) và lựa chọn, bổ sung trên cơ sở tham khảo khuôn dạng chứng thư số của một số nước.

TCVN 8066:2009 do Viện Khoa học Kỹ thuật Bưu điện biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Công nghệ thông tin – Khuôn dạng chứng thư số

Information Technology – Digital Certificate Format

1. Phạm vi áp dụng

Tiêu chuẩn này quy định về khuôn dạng chứng thư khoá công khai, hay còn gọi là chứng thư số, được sử dụng trong dịch vụ chứng thực chữ ký số.

Tiêu chuẩn này không bao hàm khuôn dạng của chứng thư thuộc tính.

Khuôn dạng chứng thư số trong Tiêu chuẩn này áp dụng phù hợp cho các tổ chức chứng thực tại Việt Nam, bao gồm tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia, tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng, tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng.

2. Tài liệu viện dẫn

ITU-T Recommendation X.509 (8/2005) | ISO/IEC 9594-8, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks *(Công nghệ thông tin - Kết nối các hệ thống mở - Thư mục: Khuôn dạng chứng thư khoá công khai và chứng thư thuộc tính).*

IETF - RFC 3280, Internet X.509 Public Key Infrastructure (April 2002), Certificate and Certificate Revocation List (CRL) Profile *(Cơ sở hạ tầng khoá công khai X.509 trên môi trường Internet, Mẫu chứng thư và danh sách chứng thư bị thu hồi).*

IETF - RFC 3281, Internet X.509 Public Key Infrastructure (April 2002), An Internet Attribute Certificate Profile *(Cơ sở hạ tầng khoá công khai X.509 trên môi trường Internet).*

3. Thuật ngữ và định nghĩa

Trong tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa sau đây:

3.1

Chứng thư thuộc tính (AC - Attribute Certificate)

Một cấu trúc dữ liệu gắn kết một số giá trị thuộc tính với thông tin định danh của người sở hữu nó. Chứng thư thuộc tính được ký số bởi tổ chức cấp chứng thư thuộc tính.

3.2

Tổ chức cấp chứng thư khoá công khai (CA - Certification Authority)

Tổ chức có trách nhiệm phát hành các chứng thư khoá công khai.

3.3