

658.8
NG-44
2004

Ts. Nguyễn Nam Hải - Ks. Đào Thị Hồng Vân - Ts. Phạm Ngọc Thụy

CHỨNG THỰC TRONG THƯƠNG MẠI ĐIỆN TỬ

QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ
Số VV-D2/6875



NHÀ XUẤT BẢN KHOA HỌC VÀ KỸ THUẬT
HÀ NỘI

MỤC LỤC

Chương I: Các hiểm hoạ đối với an toàn thương mại điện tử.....	4
1.1 Thương mại điện tử là gì ?.....	4
1.2 Các hiểm hoạ đối với an toàn thương mại điện tử.....	12
1.2.2 Các hiểm hoạ đối với sở hữu trí tuệ.....	16
1.2.3 Các hiểm hoạ đối với thương mại điện tử.....	17
1.2.4 CERT.....	32
1.3 Tóm tắt.....	32
Chương II: Những mục tiêu của an toàn thương mại điện tử..	35
2.1 Giới thiệu.....	35
2.2 Bảo vệ các tài sản thương mại điện tử.....	35
2.3 Bảo vệ sở hữu trí tuệ.....	37
2.4 Bảo vệ các máy khách.....	38
2.5 Bảo vệ các kênh thương mại điện tử.....	45
2.6 Đảm bảo tính toàn vẹn giao dịch.....	56
2.7 Bảo vệ máy chủ thương mại.....	59
2.8 Tóm tắt.....	63
Chương III: Một số kỹ thuật an toàn cho thương mại điện tử.....	65
3.1 Mã hoá đối xứng.....	65
3.2 Mã hoá khoá công khai.....	67
3.2.1 Các nguyên lý của các hệ mật khoá công khai.....	67
3.2.2 Quản lý khoá.....	75
3.3 Xác thực thông báo và các hàm băm.....	84
3.3.1 Các yêu cầu xác thực.....	84

3.3.2 Các hàm xác thực.....	85
3.4 Chữ ký số.....	96
2.4.1 Các yêu cầu.....	95
3.4.2 Chuẩn chữ ký số.....	99
3.5 Tóm tắt.....	103
Chương IV: Chứng chỉ điện tử.....	105
4.1 Giới thiệu về các chứng chỉ khoá công khai.....	105
4.1.1 Đường dẫn chứng thực.....	108
4.1.2 Thời hạn hợp lệ và việc thu hồi.....	110
4.1.3. Các mối quan hệ mang tính pháp lý.....	110
4.2 Quản lý cặp khoá công khai và khoá riêng.....	111
4.2.1 Quá trình sinh cặp khoá.....	112
4.2.2 Bảo vệ khoá riêng.....	113
4.2.3 Cập nhật cặp khoá.....	113
4.3 Phát hành các chứng chỉ.....	116
4.3.1 Xin cấp một chứng chỉ.....	116
4.3.2 Quá trình tạo chứng chỉ.....	117
4.3.3 Xác thực chủ thể.....	117
4.3.4 Cơ quan đăng ký địa phương.....	118
4.3.5 Cập nhật chứng chỉ.....	119
4.4 Phân phối chứng chỉ.....	120
4.4.1 Chứng chỉ kèm theo chữ ký.....	120
4.4.2 Phân phối thông qua dịch vụ thư mục.....	120
4.4.3 Các giải pháp phân phối khác.....	122
4.5 Khuôn dạng chứng chỉ X.509.....	122
4.5.1 Khuôn dạng chứng chỉ cơ bản.....	123
4.5.2 Tên trong X.509.....	124

4.5.3	Đăng ký đối tượng.....	126
4.5.4	Khuôn dạng chứng chỉ X.509 mở rộng (v.3).....	129
4.5.5	Đặt tên trong phiên bản 3 của X.509.....	132
4.5.6	Các trường mở rộng chuẩn của chứng chỉ.....	134
4.5.7	Ký hiệu và mã của ASN.1.....	138
4.6	Việc thu hồi chứng chỉ	138
4.6.1	Yêu cầu thu hồi.....	138
4.6.2	Danh sách các chứng chỉ bị thu hồi (CRL).....	139
4.6.3	Việc quảng bá các CRL.....	141
4.6.4	Sự thu hồi ngay lập tức	142
4.6.5	Dòng thời gian xử lý thu hồi.....	144
4.7	CRL theo X.509	146
4.7.1	Khuôn dạng CRL	147
4.7.2	Các trường mở rộng chung	149
4.7.3	Các điểm phân tán CRL.....	150
4.7.4	Các Delta-CRL.....	152
4.7.5	Các CRL gián tiếp.....	152
4.7.6	Treo chứng chỉ.....	153
4.8	Cập khoá và thời hạn hợp lệ của chứng chỉ	154
4.8.1	Các cập khoá liên quan đến mã hoá.....	155
4.8.2	Các cập khoá dùng cho ký số.....	155
4.8.3	Cập khoá dùng cho mục đích ký của CA.....	157
4.9	Chứng thực thông tin uỷ quyền.....	157
4.9.1	Thông tin uỷ quyền trong các chứng chỉ X.509	158
4.9.2	Các chứng chỉ thuộc tính.....	159
4.9.3	Các chứng chỉ thuộc tính đặc quyền	160
4.9.4	Cơ sở hạ tầng an toàn được phân tán đơn giản	162

4.9.5 Cơ sở hạ tầng khoá công khai đơn giản	163
4.10 Tóm tắt	164
Chương V: Cơ sở hạ tầng khoá công khai	166
5.1 Các yêu cầu	166
5.2 Các cấu trúc quan hệ của CA	168
5.2.1 Cấu trúc phân cấp tổng quát	168
5.2.2 Cấu trúc phân cấp với liên kết bổ sung	171
5.2.3 Cấu trúc phân cấp trên - xuống	172
5.2.4 Cơ sở hạ tầng PEM	173
5.2.5 Các cây phân cấp	176
5.2.6 Mô hình chứng thực của PGP	177
5.2.7 Mô hình tin cậy ràng buộc tăng dần	179
5.2.8 Chứng chỉ được ký chéo nhiều lần	183
5.3 Các chính sách của chứng chỉ X.509	184
5.3.1 Khái niệm chính sách chứng chỉ	184
5.3.2 Mở rộng Các chính sách chứng chỉ (Certificate Policies)	186
5.3.3 Trường mở rộng Ảnh xạ chính sách (Policy Mapping)	188
5.3.4 Mở rộng Các ràng buộc chính sách (Policy Constraints)	189
5.3.5 Các nội dung của một chính sách chứng chỉ	190
5.4 Các ràng buộc tên X.509	191
5.5 Tìm các đường dẫn chứng thực và phê chuẩn	193
5.5.1 Tìm đường dẫn chứng thực	193
5.5.2 Phê chuẩn đường dẫn chứng thực	196
5.6 Các giao thức quản lý chứng chỉ	197
5.7 Ban hành luật	197
5.7.1 Công nghệ	198
5.7.2 Phạm vi và chi tiết	199

5.7.3 Các văn bản và chữ ký.....	199
5.7.4 Chất lượng và các chuẩn của CA.....	200
5.7.5 Các chuẩn về thuê bao.....	201
5.7.6 Chia nhỏ trách nhiệm pháp lý.....	201
5.8 Hai mô hình PKI.....	202
5.8.1 Cơ sở hạ tầng SET.....	202
5.8.2 Cơ sở hạ tầng DoD MISSI.....	206
Chương VI: Quy định Hoạt động chứng thực.....	210
6.1 Khái niệm.....	210
6.2 Biểu diễn một CPS.....	212
6.3 Nền tảng cho các hoạt động chứng thực.....	214
6.4 Các thủ tục xin cấp chứng chỉ.....	223
6.5 Phát hành chứng chỉ.....	226
6.6 Chấp nhận chứng chỉ.....	227
6.7 Sử dụng chứng chỉ để kiểm tra chữ ký số.....	228
6.8 Việc treo và huỷ bỏ chứng chỉ.....	230
6.9 Sự đảm bảo và giới hạn trách nhiệm pháp lý.....	231
6.10 Các điều khoản linh tinh.....	233
6.11 Sự tiến triển không ngừng.....	234
6.12 Tóm tắt.....	236
Chương VII: Luật chữ ký điện tử.....	240
7.1 Luật mẫu về Chữ ký điện tử của UNCITRAL.....	240
7.2 Chữ ký số.....	246
Phụ lục: Định nghĩa chính sách chứng chỉ CANADA.....	253
Lời nói đầu.....	253
Định nghĩa.....	254
Danh sách các từ viết tắt.....	254

Phần I: Chính sách chứng chỉ dành cho các ứng dụng chữ ký số	256
1 Giới thiệu	256
1.1 Tổng quan	256
1.2 Nhận dạng	256
1.3 Cộng đồng và khả năng áp dụng	257
1.3.1 Các cơ quan chứng thực	257
1.3.2 Các cơ quan đăng ký	257
1.4 Các chi tiết liên hệ	259
1.4.2 Người liên hệ	259
1.4.3 Người quyết định khả năng phù hợp của CPS với chính sách	259
2 Các Điều khoản chung	259
2.1 Trách nhiệm pháp lý	259
2.2 Các nghĩa vụ	261
2.3 Trách nhiệm tài chính	263
2.4 Việc Làm sáng tỏ và sự bắt buộc tuân theo	263
2.5 Lệ phí	264
2.6 Công bố và kho lưu giữ	264
2.7 Kiểm toán theo yêu cầu	265
2.8 Tính bí mật	266
2.9 Quyền sở hữu trí tuệ	266
3. Nhận dạng và xác thực	266
3.1 Đăng ký ban đầu	266
3.1.2 Yêu cầu đặt tên có nghĩa	266
3.1.3 Các nguyên tắc trong việc làm sáng tỏ các dạng tên	267
3.1.4 Tính duy nhất của các tên	267
3.1.5 Các thủ tục giải quyết tranh chấp yêu cầu tên	267

3.1.6 Sự công nhận, xác thực và vai trò của nhân hiệu đăng ký trong I&A.....	267
3.1.7 Phương pháp chứng minh quyền sở hữu đối với khoá riêng.....	267
3.1.8 Xác thực định danh của tổ chức.....	267
3.1.9 Xác thực định danh của cá nhân.....	267
3.2 Thay thế khoá định kỳ.....	268
3.3 Thay thế khoá sau khi huỷ bỏ.....	268
3.4 Yêu cầu huỷ bỏ.....	268
4. Các yêu cầu hoạt động.....	268
4.1 Xin cấp chứng chỉ.....	269
4.2 Phát hành chứng chỉ.....	269
4.3 Chấp nhận chứng chỉ.....	269
4.4 Treo và huỷ bỏ các chứng chỉ.....	269
4.5 Các thủ tục kiểm toán an toàn.....	270
4.6 Lưu trữ các bản ghi.....	271
4.7 Thay đổi khoá.....	272
4.8 Tình trạng lộ và khôi phục sau thảm hoạ.....	272
4.9 Kết thúc hoạt động của CA.....	272
5. các kiểm soát an toàn cá nhân, vật lý và thủ tục.....	272
5.1 Các kiểm soát an toàn vật lý.....	272
5.1.1 Các kiểm soát an toàn vật lý dành cho CA.....	272
5.1.2 Các kiểm soát an toàn vật lý dành cho RA.....	273
5.1.3 Các kiểm soát an toàn vật lý dành cho thực thể cuối.....	274
5.2 Các kiểm soát thủ tục.....	274
5.2.1 Các tập đặc quyền tin cậy.....	274
5.2.2 Số lượng người yêu cầu/ nhiệm vụ.....	276

5.2.3 Việc xác thực và nhận dạng cho từng tập đặc quyền	276
5.3 Các kiểm soát an toàn cá nhân	276
5.3.1 Các kiểm soát an toàn cá nhân dành cho CA	276
5.3.2 Các kiểm soát an toàn cá nhân dành cho RA	277
5.3.3 Các kiểm soát an toàn cá nhân dành cho thực thể cuối	277
6. Các kiểm soát an toàn kỹ thuật	277
6.1 Sinh và cài đặt cặp khoá	277
6.1.1 Sinh cặp khoá	277
6.1.2 Chuyển giao khoá riêng cho thực thể	278
6.1.3 Chuyển giao khoá công khai cho người phát hành chứng chỉ	278
6.1.4 Chuyển giao khoá công khai của CA cho người dùng	278
6.1.5 Kích thước khoá	278
6.1.6 Sinh các tham số khoá công khai	278
6.1.7 Kiểm tra chất lượng tham số	278
6.1.8 Sinh khóa phần mềm/phần cứng	278
6.1.9 Mục đích sử dụng khoá (Như X.509 phiên bản 3)	278
6.2 Bảo vệ khoá riêng	278
6.2.1 Các chuẩn dành cho mô đun mật mã	278
6.2.2 Khoá riêng có nhiều người kiểm soát	279
6.2.3 Lưu trữ, sao lưu dự phòng và uỷ nhiệm khoá riêng	279
6.2.4 Khoá riêng được sử dụng trong mô đun mật mã	279
6.2.5 Phương pháp huỷ bỏ khoá riêng	279
6.3 Các khía cạnh khác liên quan tới việc quản lý cặp khoá	279
6.3.1 Lưu trữ khoá công khai	279
6.3.2 Khoảng thời gian sử dụng khoá công khai và khoá riêng	279
6.4 Dữ liệu kích hoạt	280

6.5 Các kiểm soát an toàn máy tính	280
6.6 Các kiểm soát kỹ thuật đối với chu kỳ tồn tại	280
6.6.1 Các kiểm soát phát triển hệ thống	280
6.6.2 Các kiểm soát quản lý an toàn	281
6.7 Các kiểm soát an toàn mạng	281
6.8 Các kiểm soát kỹ thuật mật mã	282
6.9 Đảm bảo an toàn máy tính	282
6.10 Đảm bảo an toàn chu kỳ tồn tại	282
7. Các Khái lược của chứng chỉ và CRL	282
7.1 Các Khái lược và phiên bản của chứng chỉ	283
7.2 Tên đối tượng của chính sách	283
7.3 Các tên đối tượng của thuật toán ký	283
7.4 Sử dụng của các trường tên	283
7.5 Các ràng buộc tên và dạng tên dành cho các ràng buộc tên	283
7.6 Các trường mở rộng của chứng chỉ và tính thiết yếu của chúng	283
7.7 Sử dụng của các ràng buộc chính sách	284
7.8 Các qualifier của chính sách	284
7.9 Xử lý ngữ nghĩa cho mở rộng chính sách chứng chỉ thiết yếu	284
7.10 Số lượng phiên bản CRL	284
7.11 CRL, các mở rộng của CRL entry và tính thiết yếu của chúng	284
8. Quản lý đặc tả	284
8.1 Các thủ tục thay đổi đặc tả	284
8.1.1 Các mục có thể thay đổi không cần thông báo	284
8.1.2 Các thay đổi cần thông báo	284
8.1.3 Các mục thay đổi yêu cầu một chính sách mới	285

8.2 Việc công bố và thông báo các chính sách.....	285
8.2.1 Các mục không được công bố trong CPS.....	285
8.2.2 Việc phân phối định nghĩa chính sách chứng chỉ và CPS.....	285
8.3 Các thủ tục phê chuẩn CPS.....	286
Phần II: Chính sách chứng chỉ dành Cho các ứng dụng thiết lập khoá mã.....	287
1. Giới thiệu.....	287
1.1 Tổng quan.....	287
1.2 Nhận dạng.....	288
1.3 Cộng đồng và khả năng áp dụng.....	288
1.3.1 Khả năng áp dụng.....	288
2. Các điều khoản chung.....	288
2.1 Tính bí mật.....	288
3. Nhận dạng và xác thực.....	289
3.1 Đăng ký ban đầu.....	289
3.1.1 Phương pháp chứng minh quyền sở hữu đối với khoá riêng.....	289
4. Các yêu cầu hoạt động.....	289
5. Các kiểm soát an toàn cá nhân, vật lý và thủ tục.....	289
6. Các kiểm soát an toàn kỹ thuật.....	289
6.1 Sinh và cài đặt cặp khoá.....	289
6.1.1 Sinh cặp khoá.....	289
6.1.2 Chuyển giao khoá riêng cho thực thể.....	289
6.1.3 Kích thước khoá.....	290
6.1.4 Sinh các tham số khoá công khai.....	290
6.1.5 Các mục đích sử dụng khoá (Như X.509 phiên bản 3).....	290
6.2 Bảo vệ khoá riêng.....	290
6.2.1 Ủy nhiệm khoá riêng.....	290

6.2.2 Sao lưu dự phòng khoá riêng.....	290
6.2.3 Lưu trữ khoá riêng	290
6.2.4 Khoá riêng được sử dụng trong mô đun mật mã	290
6.3 Các khía cạnh khác liên quan tới việc quản lý cặp khoá ...	290
6.3.1 Lưu trữ khoá công khai	290
6.3.2 Khoảng thời gian sử dụng của khoá công khai và khoá riêng	291
7. Các khái lược của chứng chỉ và CRL.....	291
7.2 Tên đối tượng của chính sách	291
8. Quản lý đặc tả	291
Các từ viết tắt và một số khái niệm	297
Tài liệu tham khảo.....	304