Chữ ký số trong thẻ thông minh và ứng dụng xác thực : Luận văn ThS /

Lương Việt Nguyên ; Nghd. : PGS.TS. Trịnh Nhật Tiến . - H. : ĐHCN, 2008 . - 152 tr. + CD-ROM

Tóm tắt: Tổng quan về thẻ thông minh: về cấu trúc vật lý, hệ điều hành, quá trình sản xuất…của smart card để phát triển các ứng dụng cho thẻ thông minh. Trình bày khái niệm cơ bản về hạ tầng mật mã khóa công khai (PKI) và phân tích các cơ sở khoa học của PKI đồng thời đưa ra các giải pháp xây dựng và thẻ xác nhận theo chuẩn X.509, PKI và thẻ thông minh. Nghiên cứu những vấn đề an toàn, rủi ro và các giải pháp tích hợp… khi ứng dụng thẻ thông minh trong đào tạo trực tuyến. Phân tích và đánh giá các công cụ dùng thẻ PKI trong hệ thống đào tạo trực tuyến và các chủ thể tham gia vào hệ thống thẻ này

Chương 1: **TỔNG QUAN VỀ THẺ THÔNG MINH 1**

1.1. GIỚI THIỆU THẺ THÔNG MINH ..... Ì

1.1.1. ưu nhược điểm và tính khả thi thẻ thông minh 3

1.1.1.1. Ưu Mần: *..... 3*

1.1.1.2. Nhược điểm: *..... 4*

1.1.1.3. Tỉnh khả thi: *..... 4*

1.1.2. Phân loại thẻ 5

1.1.3. Các chuẩn cho Smart Card 8

1 .2. CẤU TẠO THẺ THÔNG MINH ..... lo

1.2.1. Cấu trúc vật lý ..... lo

1.2.1.1. Các điếm tiếp xúc *..... lo*

1.2.1.2. Bộ xử lý trung tâm trong thẻ thông minh ..... / /

1.2.1.3. Bộ đồngxửlý trong thẻ thông minh *..... li*

1.2.1.4. Hệ thống bộ nhớ của thẻ thông minh 12

1.2.2. Giao tiếp truyền thông với thẻ thông minh 12

1.2.2.1. Thiết bị chấp nhận thẻ và các úng dụng máy chủ *..... 12*

1.2.2.2. Mô hình truyền thông với thẻ thông minh *..... 13*

1.2.2.3. Giao thức APDU 13

1.2.2.4. Mã hoa bit (bit encoding) *..... 15*

1.2.2.5. Giao thức TPDU 15

1.2.2.6. Thông đẹp trả lời để xác lập lại (ATR) *..... 17*

1.2.3. Hệ điều hành thẻ thông minh 17

1.2.4. Các File hệ thống trong thẻ thông minh 17

1.2.4.1. Thưmục gốc (Master File - MF) 17

1.2.4.2. Thư mục chuyên dụng (Dedicated File - DF) 18

1.2.4.3. File cơbản (Elementary File - EF) 18

1.2.5. Truy cập File 19

7.2.5.7. Định danh file 19

1.2.5.2. Các phương thức lựa chọn file 19

1.2.5.3. Điều kiện truy cập file 20

1.2.5.4. Lệnh thao tác với thẻ 21

1.2.6. Quá trình sản xuất một Smart Card 24

1.3. ỨNG DỤNG THẺ THÔNG MINH 25
1.3.1. Phát triển ứng dụng cho Smart Card 25
1.3.1.1. Quy trình phát triển ứng dụng cho Smart Card. *25*
1.3.1.2. Các công cụ phát triển ứng dụng cho Smart Card *26*
1.3.1.3. Công cụ cho ứng dụng phửi thẻ *26*
1.3.2. ứng dụng phía thiết bị đọc thẻ (reader) 27
1.3.2.1. Các giao diện ứng dụng chuẩn phửi reader *27*
1.3.2.2. Chuẩn PC/SC *28*
1.3.2.3. Kiến trúc PC/SC *28*
1.3.2.4. ICC Resource Manager *30*
1.3.2.5. ICCSP *32*
1.3.2. é *Các chuẩn khác* *33*
1.3.3. ứng dụng phía thẻ 34
1.3.3.1. Các khía cạnh trong phát triển ứng dụng. *34*
1.3.3.2. Tập các hàm API. *35*
1.3.4. Một số ứng dụng trong thẻ thông minh 37
1.3.4.1. Thẻ thông minh trong hệ thống thu lệ phí (cầu, đường) điện tử. *37*
1.3.4.2. Thẻ thông minh trong chữký so (Digital Signature) *38*
1.3.4.3. Thẻ thông minh trong hệ thống trả tiền điện tử *40*
1.4. TÓM TẮT CHƯƠNG 42
Chương 2: TÒNG QUAN VỀ HẠ TÀNG MẬT MÃ KHÓA CÔNG KHAI (PKI) 43
2.1. KHÁI NIỆM VỀ PKI 43
2.2. Cơ SỞ KHOA HỌC VỀ PKI 44
2.2.1. Các thành phần kỹ thuật cơ bản của PKI 44
2.2.1.1. Mã hóa *44*
2.2.1.2. Ký số *48*
2.2.1.3. Chứng chỉ số *59*
2.2.2. Lợi ích của chứng chỉ số 61
2.2.2.1. Đảm bảo tính xác thực *61*
2.2.2.2. Mã hóa *62*
2.2.2.3. Chống giả mạo *62*
2.2.2.4. Chống chối cãi nguồn gốc *62*
2.2.2.5. Đảm bảo phần mần *62*
2.2.2.6. Phân phối khóa an toàn *63*
2.2.2.7. Bảo mật Website *64*
2.2.2.8. Xử lý độc lập tại máy khách *64*

2.2.3. Công nghệ để xây dựng PKI và giao thức....65

2.2.3.1. Công nghệ OpenCA 65

2.2.3.2. Công nghệ SSL 66

2.2.3.3. Giao thức truyền tin an toàn tầng liên kết dữliệu (Data Link) 70

2.2.3.4. Giao thức truyền tin an toàn tầng itng dụng(Applỉcation) 72

2.2.3.5. Một số công nghệ bảo mật và an toàn thông tin trên thế giới.... 74

2.3. GIẢI PHÁP XÂY DỰNG PKI 75

2.3.1. Hành lang pháp lý để xây dựng và ứng dụng PKI....75

2.3.2. Giải pháp công nghệ xây dựng PKI hiện nay....77

2.4. CÁC ĐỐI TƯỢNG cơ BẢN CỦA HỆ THỐNG PKI 78

2.4.1. Chủ thể và các đối tượng sử dụng....78

2.4.2. Đối tượng quản lý thẻ xác thực 79

2.4.3. Đối tượng quản lý đăng ký thẻ xác thực 80

2.5. CÁC HOẠT ĐỘNG cơ BẢN TRONG HỆ THỐNG PKI 81

2.5.1. Mô hình tổng quát của hệ thống PKI....81

2.5.1.1. Thiết lập các thẻ xác thực .... SI

2.5.1.2. Khởi tạo các EE....82

2.5.2. Các hoạt động liên quan đến thẻ xác thực 82

2.5.2.1. Đăng ký và xác thực ban đầu 82

2.5.2.2. Cập nhật thông tin về cặp khóa....82

2.5.2.3. Cập nhật thông tin về thẻ xác thục....83

2.5.2.4. Cập nhật thông tin về cặp khóa của CA 83

2.5.2.5. Yêu cầu xác thục ngang hàng....83

2.5.2.6. Cập nhật thẻ xác thục ngang hàng....83

2.5.3. Phát hành thẻ và danh sách thẻ bị hủy bỏ 84

2.5.4. Các hoạt động phục hồi.... 84

2.5.5. Các hoạt động hủy bỏ.... 84

2.6. NHỮNG VẤN ĐỀ cơ BẢN TRONG XÂY DỰNG HỆ THỐNG PKI.... 85

2.6.1. Các mô hình tổ chức hệ thống CA.... 85

2.6.1.1. Kiến trúc phân cấp.... 85

2.6.1.2. Kiến trúc hệ thống PKI mạng lưới....87

2.6.1.3. Kiến trúc danh sách tin cậy 88

2.6.2. Những chức năng bắt buộc trong quản lý PKI....90

2.6.2.1. Khởi tạo CA gốc.... 90

2.6.2.2. Khởi tạo các CA thứ cấp.... 90

2.6.2.3. Cập nhật khóa của CA gốc 91
2.6.2.4. Tạo lập CRL 91
2.6.2.5. Yêu cầu về thông tin hệ thống PK1 91
2.6.2.6. Xác thực ngang hàng 91
2.6.2.7. Khởi tạo các EE 92
2.6.2.8. Yêu cẩu xác thực 92
2.6.2.9. Cập nhật khóa 92
2.7. THẺ XÁC NHẬN THEO CHUẨN X.509 93
2.7.1. Khuôn Dạng Chứng Chỉ X.509 93
2.7.2. Các trường cơ bản của thẻ xác thực 94
2.7.2.1. Trường tbsCertificate 94
2.7.2.2. Trường signatureAlgorithm 95
2.7.2.3. Trường signatureValue 95
2.7.3. Cấu trúc TBS Certificate 96
2.7.3.1. Trường version 96
2.7.3.2. Trường serialNumber 96
2.7.3.3. Trường signature 97
2.7.3.4. Trường issuer 97
2.7.3.5. Trường validity 98
2.7.3.6. Trường subject 98
2.7.3.7. Trường subjectPublicKeylnfo 99
2.7.3.8. Trường uniqueldentiflers 99
2.7.3.9. Trường extensions 99
2.7Ả. Các phần mở rộng của thẻ xác thực X.509 99
2.7.4.1. Phần mở rộng Authority Key Identifier 99
2.7.4.2. Phần mở rộng Subject Key Identifier 100
2.7.4.3. Phần mở rộng Key Usage 100
2.7.4.4. Mục đích sửdụng khóa mởrộng (Extended Key Usage) 102
2.7.4.5. Phần mở rộng Private Key Usage Period. 102
2.7.4.6. Phần mở rộng Certificate Policies 102
2.7.4.7. Phần mở rộng Policy Mappings 103
2.7.4.8. Phần mở rộng Subject Alternative Name 104
2.7.4.9. Phần mở rộng Issuer Alternative Names 105
2.7.4.10. Phẩn mở rộng Subject Directory Attributes 105
2.7.4.11. Phần mở rộng Basic Constraints 105
2.7.4.12. Phần mở rộng Name Constraints 106

2.7.4.13. Phần mở rộng Policy Constraints.....106

2.7.4.14. Phần mở rộng Extended key usage field.....107

2.7.4.15. Phần mở rộng CRL Distribution Points.....108

2.7.4.16. Các trường mở rộng cho Internet.....109

2.8. PKI VÀ THẺ THÔNG MINH..... 109

2.8.1. Luật pháp..... 109

2.8.2. Mối quan hệ giữa công nghệ, ứng dụng và luật pháp..... no

2.9. TÓM TẮT CHƯƠNG..... 111

***Chương 3:* ỨNG DỤNG THẺ THÔNG MINH TRONG ĐÀO TẠO TRỰC TUYẾN...112**

3.1. GIỚI THIỆU..... 112

3.2. TỔNG QUAN HỆ THÔNG HỌC TRỰC TUYẾN (E-LEARNING)..... 113

3.3. RỦI RO LIÊN QUAN VỚI HỆ THÔNG E-LEARNING..... 115

3.4. VẤN ĐỀ AN TOÀN TRONG MÔI TRƯỜNG HỌC TRỰC TUYẾN?..... 116

3.5. GIAO DỊCH AN TOÀN TRÊN INTERNET..... 116

3.6. CÁC CHỦ THẺ THAM GIA VÀO HỆ THỐNG THẺ THÔNG MINH..... 119

3.7. GIẢI PHÁP TÍCH HỢP THẺ THÔNG MINH TRONG HỌC TRỰC TUYẾN.... 119

3.7.1. Mô hình kết hợp ngoài và mô hình kết họp trong..... 119

3.7.2. Mô hình cấp chứng chỉ đơn giản..... 121

3.7.3. Mô hình sử dụng thẻ thông minh phân bố rộng..... 121

3.8. XÁC THỰC SỬ DỤNG THẺ THÔNG MINH VÀ GIAO THỨC SSL TRONG ĐÀO TẠO TRỰC TUYẾN.....122

3.8.1. Thiết kế hệ thống đảm bảo tính bảo mật thông tin với chữ ký số kết họp giao thức SSL.....122

3.8.2. Nâng cấp thiết kế SSL bằng thẻ thông minh thương mại (Commercial Smart Card Token).....126

3.8.3. Quy trình xác thực sử dụng Ikey 2000 Token trong đào tạo trực tuyến 126

3.8.4. Sơ đồ chuyển chế độ của LMS và CMS trong quy trình xác thực.....130

3.9. TÓM TẮT CHƯƠNG.....134

***Chương 4:* THỪ NGHIỆM GIẢI PHÁP..... 135**

4.1. CÁC CÔNG CỤ DÙNG TRONG HỆ THỐNG.....135

4.1.1. Các công cụ quản trị hệ thống..... 135

4.1.1.1. Công cụ quản lý người sử dụng.....135

4.1.1.2. Công cụ tạo và quản lý chính sách.....135

4.1.1.3. Công cạ quản lý danh sách thẻ xác nhận.....136

4.1.1.4. Công cụ quản lý các sựkiện đối với hệ thống.....136

4.1.2. Lưu trữ dữ liệu 137

4.1.2.1. Lưu thông tin quản lý đối tượng sử dụng chuông trình 137

4.1.2.2. Lưu thông tin chính sách về thẻ xác nhận 137

4.1.2.3. Lưu trữ thông tin về thẻ xác nhận 138

4.1.3. Chức năng mã hoa dữ li ệu 138

4.1.3. ĩ. Sự cần thiết của chức năng 138

4.1.3.2. Định hướng xây dựng 138

4.1.3.3. Lưu đồ thuật toán thực hiện 139

4.1.4. Các thành phần của PKI/Smartcard 140

4.1.4.1. Đầu đọc thẻ thông minh 140

4.1.4.2. Thẻ Mifare dùng trong hệ thong 141

4.1.4.3. Giải pháp ứng dụng trong hệ thống đào tạo trục tuyến 142

4.1.5. Những yêu cầu về sử dụng hệ thống thẻ thông minh 144

4.2. ĐÁNH GIÁ MÔ HÌNH KẾT HỢP 145

4.3. MỘT SỐ KÉT QUẢ THỬ NGHIỆM 147

4.4. TÓM TẮT CHƯƠNG 150