

FPT Information System Ứng dụng chữ ký số cho chính phủ điện tử
Hướng đi cần thiết cho tương lai

- Tổng quan xác thực điện tử Digital signature certificate
- Các yêu cầu của một dự án xác thực điện tử
- Giải pháp đề xuất của công ty hệ thống thông tin FPT (FIS)
- Case Study
- Mô hình PKI của một số nước trên thế giới
- Thảo luận

The diagram shows three circular components arranged horizontally. The first is labeled 'Policies' with an orange background. The second is labeled 'PKI' with a blue background. The third is labeled 'Application Integration' with a green background. Arrows point from 'Policies' to 'PKI' and from 'PKI' to 'Application Integration'.

FPT Information System Các phương pháp xác thực truyền thống

The diagram shows a central green circle labeled 'Traditional Authentication method'. Four arrows point outwards to different methods: 'Dễ đoán' (Easy to guess) with a dog, 'Dễ dàng bị đánh cắp' (Easy to be stolen) with a group of people, 'Ghi ra giấy' (Written on paper) with a password slip, and 'Dễ bị bỏ khóa' (Easy to be lost) with a box. A woman is also shown with the text 'Khó nhớ' (Hard to remember).

FPT Information System Sự cần thiết của một hệ thống xác thực điện tử CA

Tình trạng/thách thức	Giải pháp xác thực điện tử dựa trên công nghệ PKI	Định hướng/yêu cầu
- Các ứng dụng truyền thống dựa trên giấy tờ đang chiếm rất nhiều thời gian, tiền bạc của doanh nghiệp - Xác thực ứng dụng: dùng user name và password, chưa đủ mạnh. - Giao dịch truyền đi: Không gắn với định danh (ID). Điều này có thể gây khó khăn trong việc xác định trách nhiệm nếu xảy ra sự cố.		- Nâng cao bảo mật của các ứng dụng điện tử. - Ký số lên thông điệp đảm bảo tính chống từ chối ở mức ứng dụng - Đưa ra cơ chế lưu lại thời điểm thông điệp được ký. - Áp dụng cho các ứng dụng nội bộ khác của tổ chức: email...

FPT Information System

Lựa chọn nào cho giải pháp xác thực điện tử?

Ba yếu tố	Chỉ phù hợp cho các ứng dụng nội bộ do giá thành triển khai lớn cũng như quản lý định danh của người sử dụng phức tạp
Hai yếu tố	Rất phù hợp để triển khai cho xác thực điện tử do khả năng tích hợp ứng dụng, bảo mật cũng như phù hợp luật giao dịch điện tử
Một yếu tố	không còn phù hợp trong môi trường điện tử do có thể bị tấn công bằng rất nhiều cách khác nhau: keylogger, brute force, phishing...

Yếu hơn ← || || → Mạnh hơn

FPT Information System

Tình hình phát triển xác thực điện tử trên thế giới

- Đài Loan:**
 - Chữ ký số được áp dụng cho hầu hết các giao dịch online.
 - Hệ thống xác thực e-Tax được bầu chọn là best practice PKI tại châu Á, tiết kiệm hàng triệu USD cho chính phủ cũng như giảm thời gian làm thủ tục khai thuế từ **3 ngày → 5 phút**.
- Hàn Quốc:**
 - Số lượng chứng thư số cấp phát tính đến cuối năm 2009 là hơn 18 triệu.
 - Các giao dịch trên mạng, thanh toán ngân hàng đều được thực hiện thông qua chứng thư số được cấp phát bởi các public CA.

FPT Information System

Tình hình áp dụng xác thực điện tử tại Việt Nam

Rất nhiều tổ chức đã có các bước đi đầu tiên áp dụng chữ ký số cho các giao dịch điện tử:

- ☐ Chứng khoán
- ☐ Ngân hàng
- ☐ Bộ Tài Chính, Tổng cục Thuế, Kho bạc Nhà nước, Tổng cục Hải quan, Tổng cục đường bộ

Khả năng áp dụng chữ ký số cho các giao dịch điện tử tại Việt Nam:

- ☐ Các ứng dụng chính phủ điện tử (e-Tax, e-Procurement, e-Bidding...).
- ☐ Hệ thống thanh toán trực tuyến (e-Commerce, e-Payment...)
- ☐ Giao dịch giữa các ngân hàng, tổ chức tài chính (Internet banking...)

Tình hình áp dụng xác thực điện tử tại Việt Nam (2)




- ❑ **Kê khai thuế qua mạng:** Mục tiêu đến năm 2015 có tối thiểu 50% doanh nghiệp kê khai thuế qua Internet
- ❑ **Kê khai hải quan điện tử:** Hiện đã triển khai tại Hải Phòng và thí điểm tại một số chi cục Hải Quan
- ❑ **Ký các văn bản ban hành :** Thành phố Hà Nội sẽ triển khai chữ ký điện tử ở 47 đơn vị

Yêu cầu của một dự án xác thực điện tử




- Khung pháp lý (quyết định 26, nghị định 59 Bộ TTTT).
- Lựa chọn công nghệ xác thực
 - PKI (public CA)
 - One time password...
- Lựa chọn ứng dụng
 - Tính cấp thiết
 - Tầm quan trọng của ứng dụng tác động lên đời sống kinh tế xã hội (e-Tax, e-Customs...)
 - Độ sẵn sàng tích hợp chữ ký số
- Xây dựng quy trình
- Đào tạo con người

Mô hình giải pháp FPT PKI Case Study



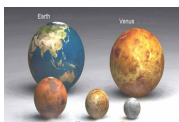
Giải pháp xác thực điện tử của FPT

- Công nghệ:
 - Hệ thống chứng thực chữ ký số công cộng FPT-CA sử dụng PKI engine đã áp dụng cho rất nhiều các hệ thống PKI lớn (National CA,...) trên thế giới.
 - FPT-CA được xây dựng theo kiến trúc PKI hiện đại, có tính mở cao.
 - Có khả năng cấp phát, xử lý hàng triệu chứng thư số.
 - Phù hợp cho các ứng dụng hiện tại: e-Tax, e-Customs... cũng như các hệ thống xác thực trong tương lai: e-Passport..
 - Tuân theo các chuẩn quốc tế: X.509, PKIX, LDAP...có thể dễ dàng mở rộng tích hợp cùng các hệ thống public CA của các nước.



Lợi ích của giải pháp xác thực điện tử FPT

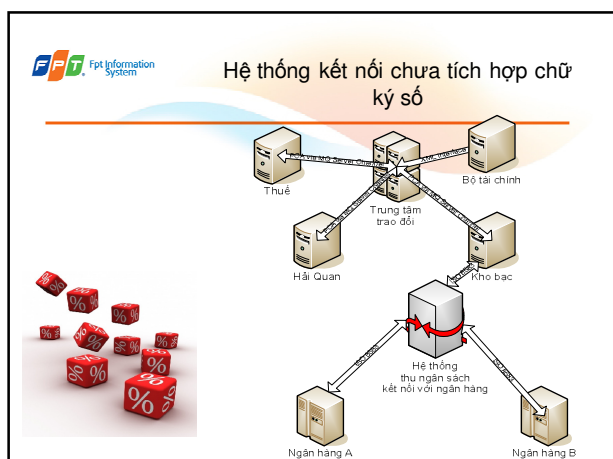
- FPT cung cấp một giải pháp toàn diện cho một hệ thống xác thực điện tử dựa trên 3 thành phần nhân tố chủ yếu:
 - Công nghệ
 - Con người
 - Quy trình
- Các cán bộ kỹ thuật của FPT đã có nhiều năm nghiên cứu, xây dựng triển khai các hệ thống PKI:
 - Hệ thống kết nối Hải quan, Kho Bạc cùng các ngân hàng
 - Hệ thống national CA Brunei...
- Phần lớn các hệ thống trao đổi thông tin giữa Bộ Tài Chính, các ngân hàng do FPT phát triển. Tích hợp chữ ký số lên các ứng dụng này đã nằm trong chiến lược phát triển dài hạn của FPT.
- FPT-CA được xây dựng để đáp ứng tất cả các quy trình chuẩn của Bộ TTTT, phù hợp cho các giao dịch điện tử theo luật định

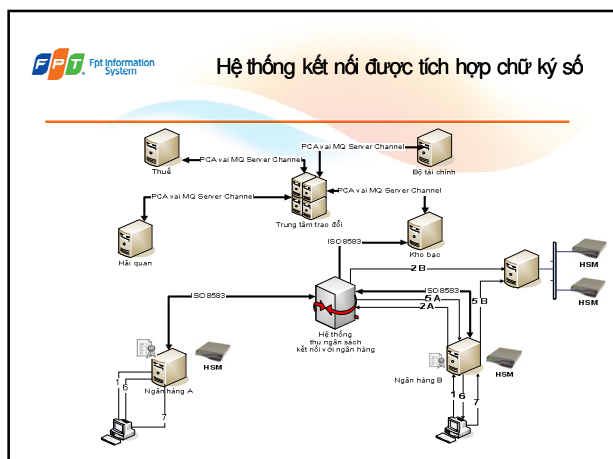


Case Study

- Bài toán:
 - Hệ thống thu ngân sách kết nối Kho Bạc đến các ngân hàng
- Yêu cầu:
 - Sau khi nhận được yêu cầu từ các ngân hàng, Kho bạc sẽ tiến hành khôi phục số thuế, ký số lên giao dịch gửi trả lại cho ngân hàng.
 - Số lượng giao dịch mà Kho bạc cần ký là rất lớn, do đó phải sử dụng phương pháp ký tự động bằng HSM.
- Giải quyết:
 - Hệ thống chứng thực chữ ký số công cộng FPT-CA
 - Hardware Security Module (HSM) AEP Keyper







FPT Fpt Information System

Case study



- Bài toán:
 - Hệ thống kết nối thanh toán liên ngân hàng
- Yêu cầu:
 - Các ngân hàng khi đăng nhập hệ thống đến hệ thống liên ngân hàng phải sử dụng PKI token
 - Tất cả các giao dịch trao đổi giữa các ngân hàng đều phải được mã hóa, ký số để đảm bảo tính bí mật.
- Giải quyết:
 - Hệ thống chứng thực chữ ký số
 - USB PKI token để lưu trữ khóa bí mật cũng như chứng thư số.

Mô hình hệ thống CA tại Nhật

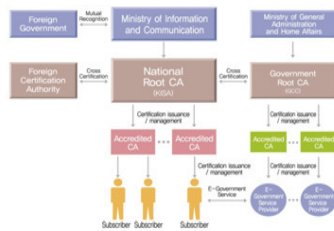
Nhật Bản sử dụng mô hình BCA nhưng được chia thành ba domain:

- ❑ Hệ thống chứng thực số dùng cho chính phủ (GPKI)
- ❑ Hệ thống chứng thực số dành cho địa phương (LGPKI)
- ❑ JPKI dành cho công dân.

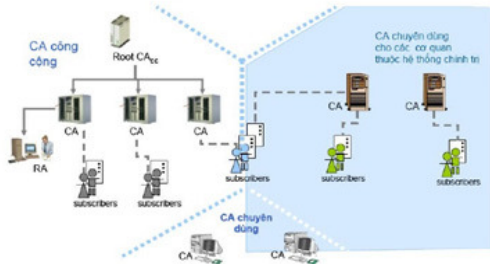


Mô hình hệ thống CA tại Hàn Quốc

- ❑ Đạt 11 triệu thuê bao vào năm 2005
- ❑ Hơn 18 triệu thuê bao vào năm 2008
- ❑ Đến nay đã có khoảng gần 20 triệu chữ số được cấp phát trên tổng số dân là 50 triệu người



Mô hình hệ thống CA tại Việt Nam





Kết luận

☺ Với việc xuất hiện ngày càng nhiều nhu cầu triển khai các dịch vụ công, việc trao đổi thông tin hành chính giữa các cơ quan lên trên hệ thống mạng, thì việc ứng dụng hạ tầng PKI cũng như chữ ký số trong Chính phủ điện tử để đảm bảo an toàn là một hướng đi cần thiết cho tương lai !



Thank you for your attention !!!