TRIỂN KHAI ỨNG DỤNG HỆ THỐNG CHỨNG THỰC SỐ CHUYÊN DÙNG CHÍNH PHỦ TẠI THÔNG TẤN XÃ VIỆT NAM

Người trình bày: Lê Quang Huy
CỤC CHỨNG THỰC SỐ & BẢO MẬT THÔNG TIN
BAN CƠ YẾU CHÍNH PHỦ

NỘI DUNG

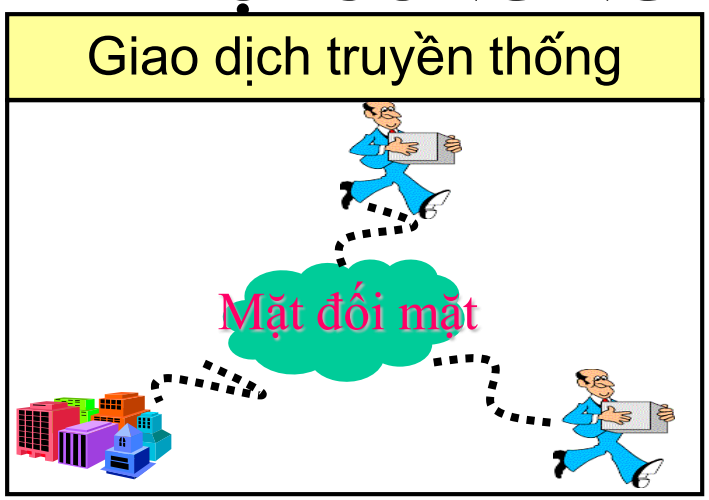
1. ĐẶT VẤN ĐỀ
2. TỔNG QUAN VỀ HỆ THỐNG CHỨNG THỰC SỐ
3. TRIỂN KHAI HỆ THỐNG CTS TRONG CQNN
4. TÓM TẮT
5. THẢO LUẬN

1. ĐẶT VẤN ĐỀ

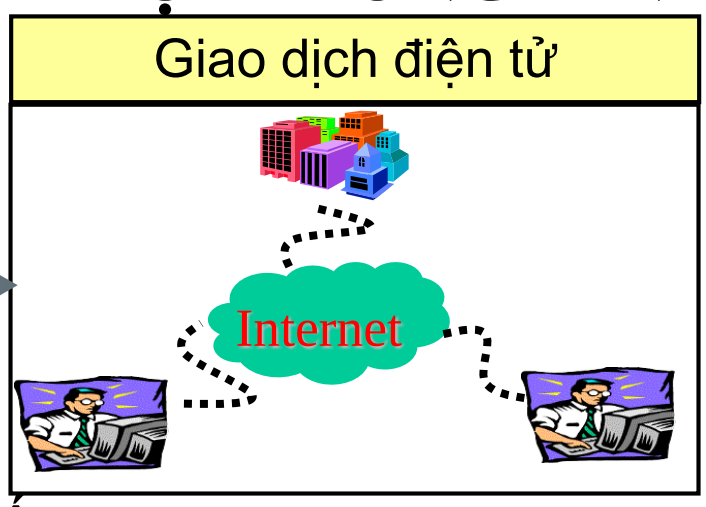
- 1.1. HIỆN TRẠNG ỨNG DỤNG CNTT TẠI CQNN
- 1.2. AN TOÀN THÔNG TIN TẠI CƠ QUAN NN
- 1.3. GIẢI PHÁP ĐẢM BẢO ATTT TRONG CQNN

1.1. HIỆN TRẠNG ỨNG DỤNG CNTT TẠI CQNN

XÃ HỘI CÔNG NGHIỆP



XÃ HỘI THÔNG TIN



Kết quả:

- PL: Hệ thống VBQPPL ứng dụng CNTT.
- Hạ tầng: Mạng TSL, Datacenter, CSDL QG.
- G2G: Website, email, hệ điều hành tác nghiệp, quản lý văn bản, xử lý hồ sơ công việc, hội nghị truyền hình…
- G2B, G2C, G2E: Website, email, DVC thiết yếu, một cửa điện tử….
- Xếp hạng : 88/193 (EGDI), 59/193 (DVC)

Hạn chế:

- Thiếu khung pháp lý đồng bộ.
- Xếp hạng ứng dụng CNTT thấp ASEAN
- CSDL quốc gia, hạ tầng thông tin chậm triển khai, bảo mật, an toàn thấp, quy mô nhỏ, kết nối, chia sẻ thông tin hẹp
- Điều hành, xử lý công việc qua mạng còn ít; số lượng DVC mức độ cao chưa nhiều.

1.2. AN TOÀN THÔNG TIN TẠI CƠ QUAN NN

- Phát hiện hơn 100.000 mã độc.
- Tỷ lệ lây nhiễm: 300%/năm.
- Loại tấn công:
  - Thay đổi giao diện (Deface),
  - Cài mã độc (Malware)
  - Lừa đảo (Phishing).
- Kiểu tấn công:
  - Lỗ hổng bảo mật.
  - Thói quen của người dùng.
- Xu hướng tấn công:
  - dữ liệu người dùng (tống tiền, thông tin cá nhân);
  - mã độc: điện thoại, thiết bị thông minh;
  - hạ tầng trọng yếu CQNN.

1.3. GIẢI PHÁP ĐẢM BẢO ATTT TRONG CQNN

Các vấn đề gây mất an toàn thông tin:

1. Ai đang giao dịch? (Xác thực)
2. Thông tin có bị xem trộm? (Bí mật)
3. Dữ liệu có bị sửa đổi ? (Toàn vẹn)
4. Chối bỏ hành động (Chống chối bỏ)

2. HỆ THỐNG CHỨNG THỰC SỐ

2.1. MẬT MÃ KHÓA CÔNG KHAI

2.2. CHỨNG THỰC SỐ

2.3. CHỨNG THƯ SỐ

2.4. CÁC THÀNH PHẦN CỦA HỆ THỐNG CTS

2.5. CÁC HOẠT ĐỘNG CHÍNH CỦA HỆ THỐNG CTS

2.6. MÔ HÌNH HOẠT ĐỘNG CỦA HỆ THỐNG CTS

2.7. ỨNG DỤNG KÝ SỐ

2.8. ỨNG DỤNG MÃ MẬT

2.9. ỨNG DỤNG XÁC THỰC, CHỐNG CHỐI BỎ

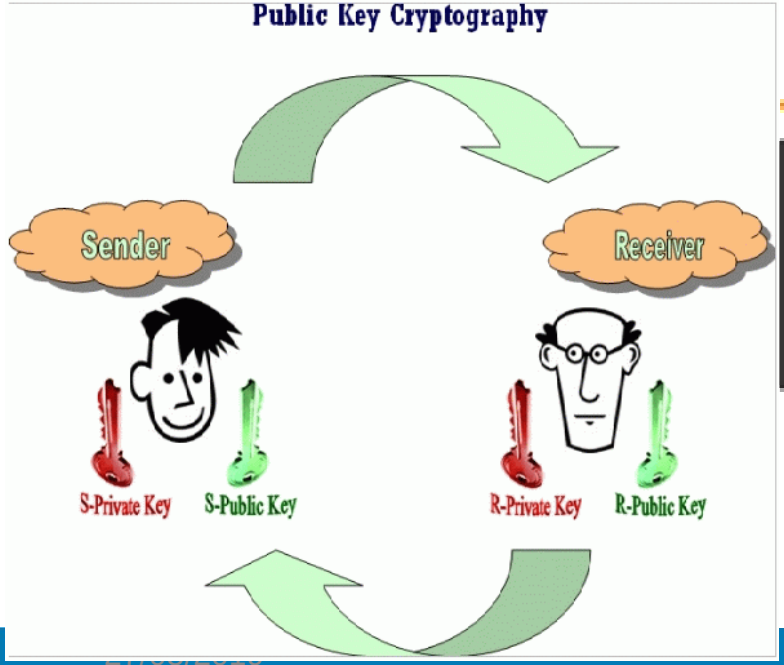
2.10. ĐẶC ĐIỂM CỦA CHỮ KÝ SỐ

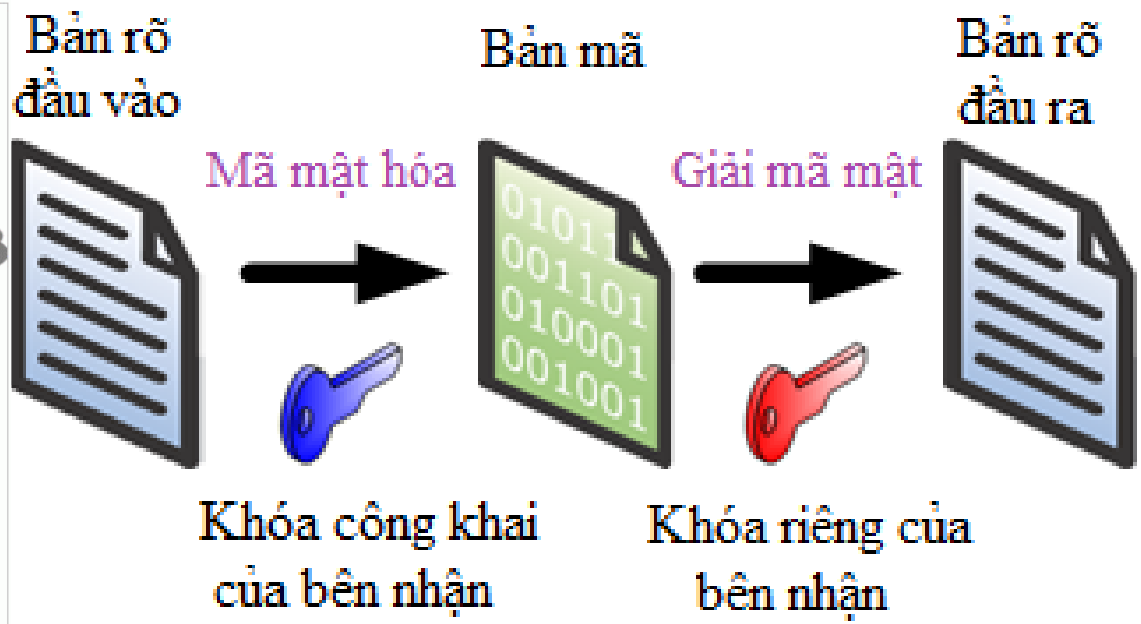
2.1. MẬT MÃ KHÓA CÔNG KHAI

Mật mã: là ngành khoa học nghiên cứu các phương pháp biến đổi thông tin để đảm bảo tính bí mật của thông tin (chuyển đổi thông tin từ dạng rõ sang dạng bí mật và ngược lại).

Mật mã bất đối xứng (mật mã khóa công khai)

- Ra đời từ cuối những năm 70.
- Sử dụng hai khóa khác biệt nhau





2.2. CHỨNG THỰC SỐ

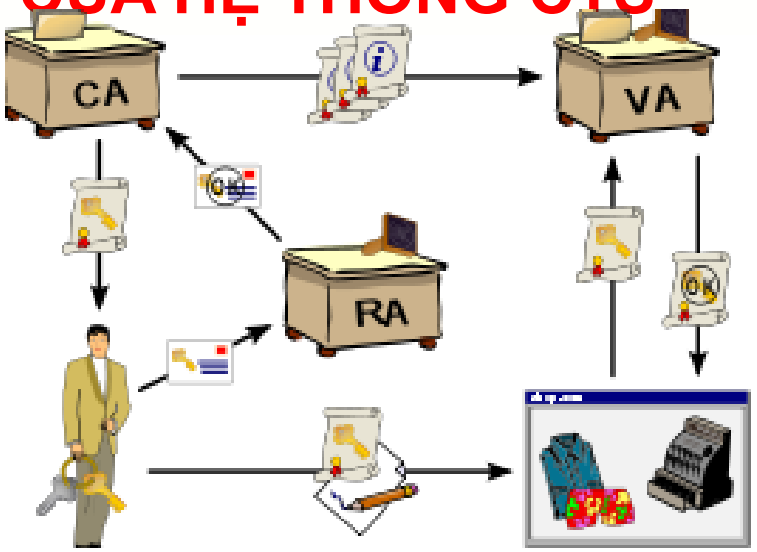
- **Chứng thực**: là việc chứng nhận một điều gì đó là đúng thông qua một phương tiện cụ thể.
- **Chứng thực số**: là việc một tổ chức có thẩm quyền (tin cậy) sử dụng các công nghệ, kỹ thuật điện tử (số) chứng nhận một cặp khóa thuộc về một chủ thể thông qua phương tiện xác định (chứng thư số).
- **Bản chất hệ thống chứng thực số**: là một hệ thống hỗ trợ cho việc áp dụng các kỹ thuật mật mã (đặc biệt mật mã khóa công khai), nhằm đảm bảo an toàn, tin cậy cho các giao dịch trong môi trường mạng.

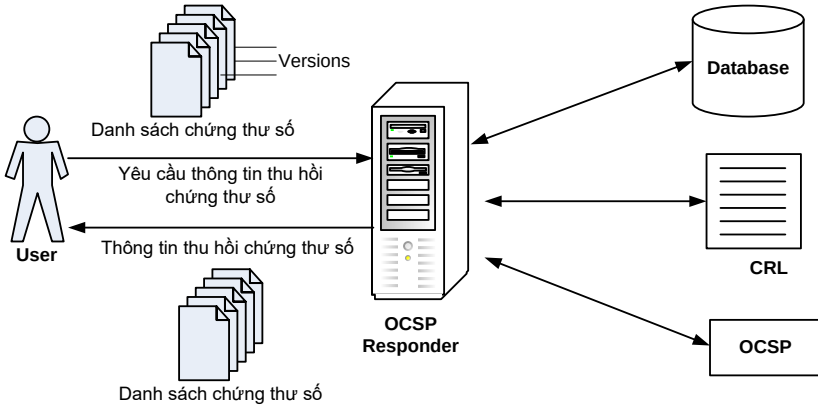
2.3. CHỨNG THƯ SỐ

- **Khái niệm:** Chứng thư số là một phương tiện thông qua nó tổ chức chứng thực chứng nhận một cặp khó thuộc về một chủ thể xác định.
- **Bản chất:** Cấu trúc dữ liệu gắn các thông tin xác định chủ thể với một khóa công khai, được ký số bởi cơ quan phát hành (Tổ chức chứng thực) và lưu trữ dưới dạng 1 tập tin (file).
- Tạo ra chứng thư số giải quyết được vấn đề xác thực cặp khóa và chống chối bỏ.
- Khóa riêng: đặt trong thiết bị lưu khóa

2.4. CÁC THÀNH PHẦN CỦA HỆ THỐNG CTS

- Hạ tầng: CA, RA, VA- cung cấp dịch vụ:
  - Chứng thực: Phát hành, thu hồi chứng thư số. Phát hành danh sách thu hồi (CRL). Quản lý vòng đời của chứng thư số sau khi phát hành.
  - Các dịch vụ (trực tuyến) nhằm khẳng định tính tin cậy và hợp lệ của chứng thư số: LDAP, CRL, OCSP…
  - Dịch vụ dấu thời gian: TimeStamp, …
- Thực thể cuối - sử dụng dịch vụ:
  - Chủ thể sở hữu chứng thư số (thuê bao)
  - Người dùng, thiết bị, tin cậy và sử dụng chứng thư số.



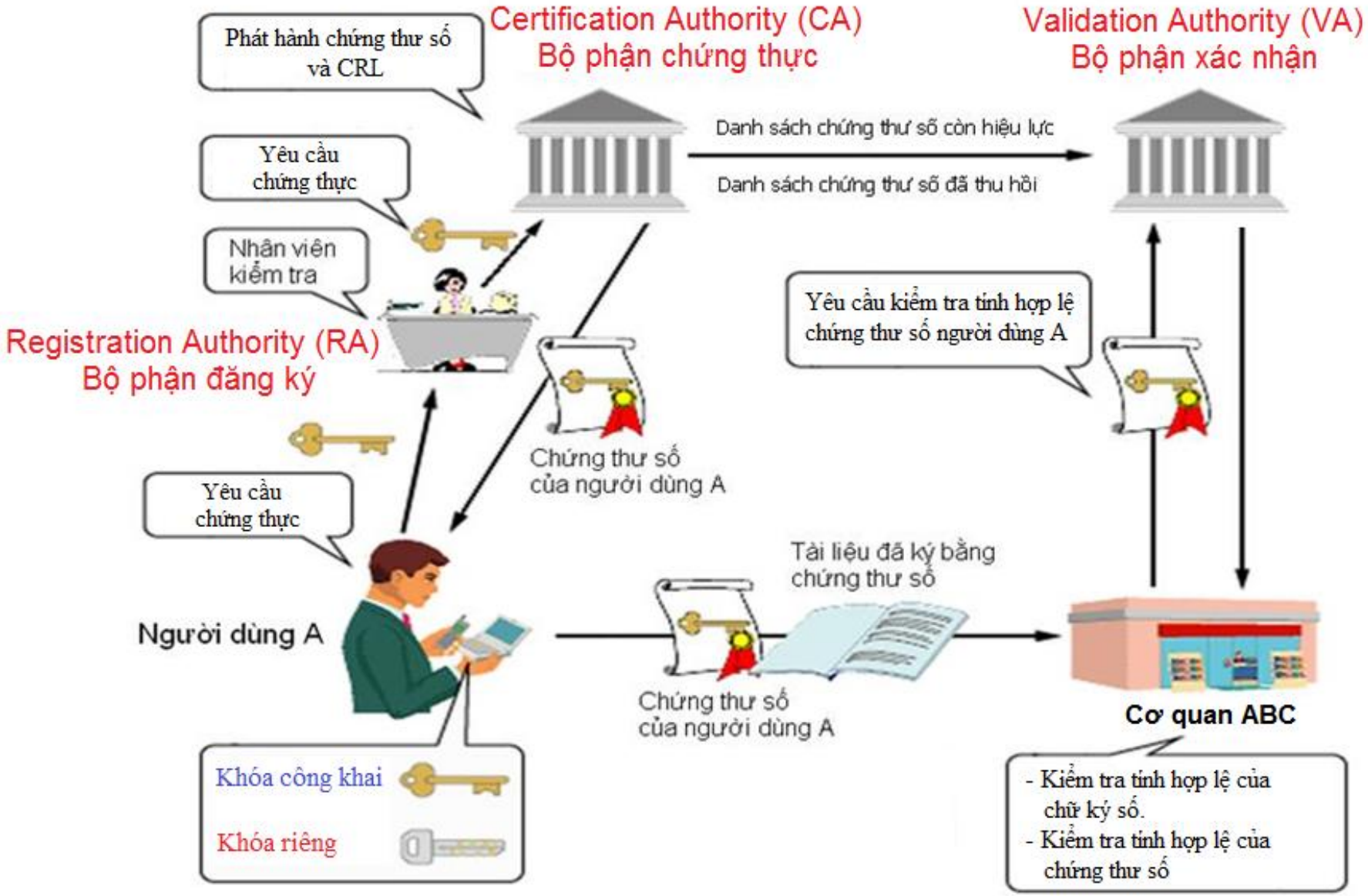


Chứng thực cặp khóa:

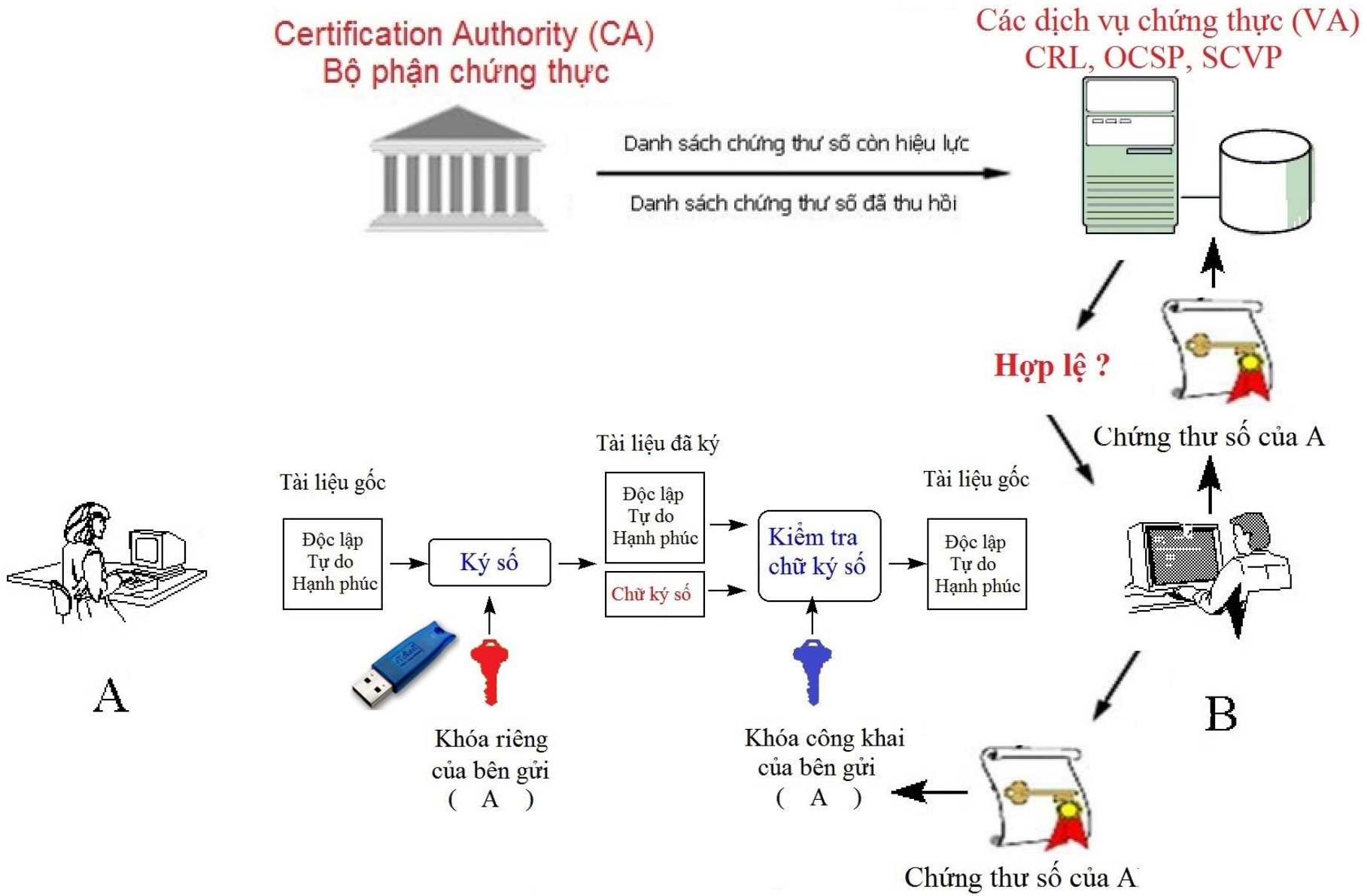
- Phát hành: cấp chứng thư số cho thuê bao.
- Gia hạn: thay đổi thời hạn sử dụng của chứng thư số.
- Tạm dừng: tạm thời làm mất hiệu lực của chứng thư số.
- Thu hồi: làm mất hiệu lực chứng thư trước khi hết hạn tự nhiên

Sử dụng chứng thư số: đảm bảo an toàn (xác thực, toàn vẹn, bí mật)

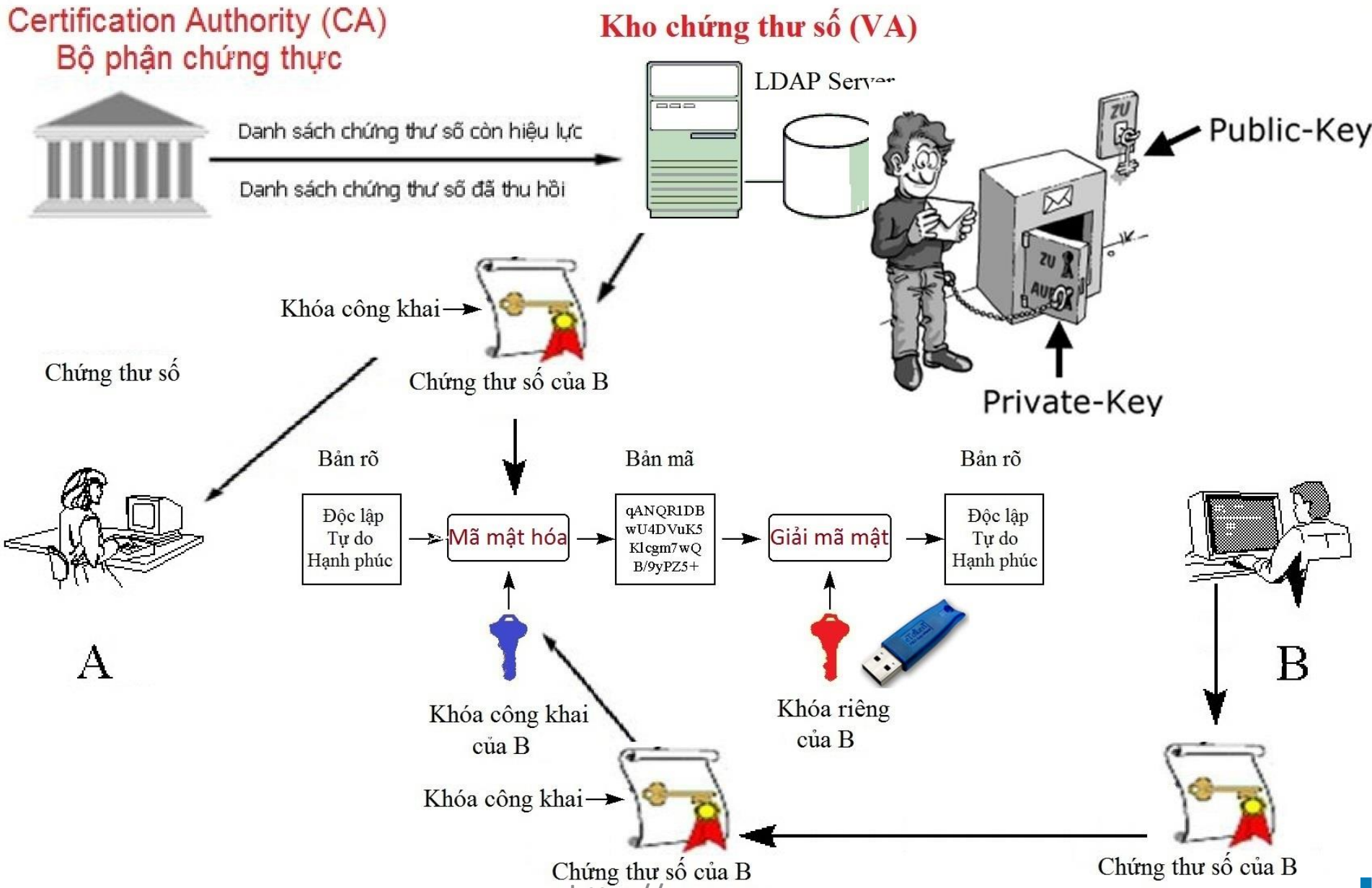
2.6. MÔ HÌNH HOẠT ĐỘNG CỦA HỆ THỐNG CTS



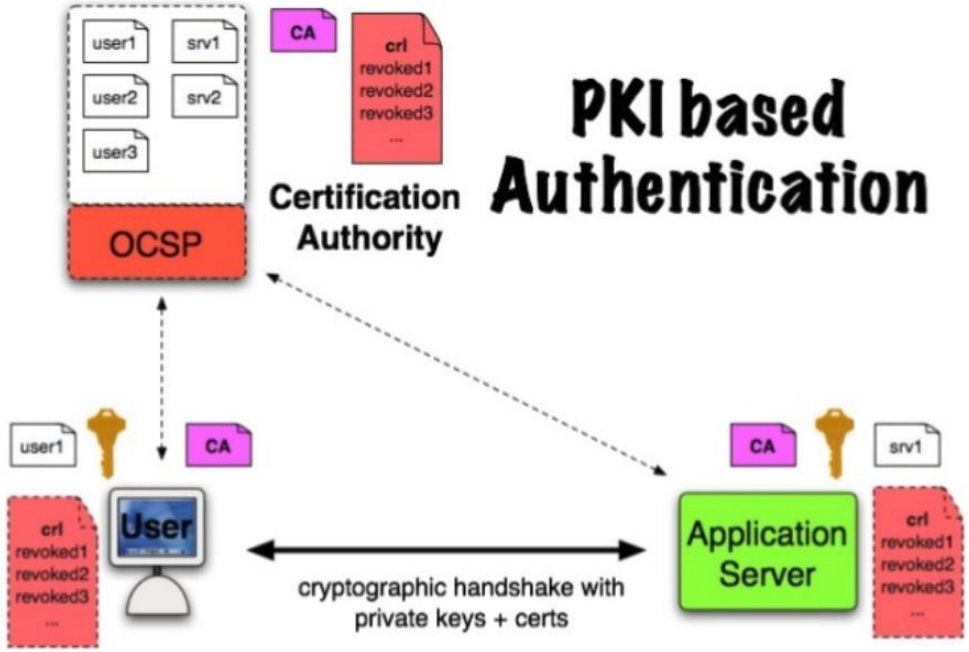
2.7. ỨNG DỤNG KÝ SỐ

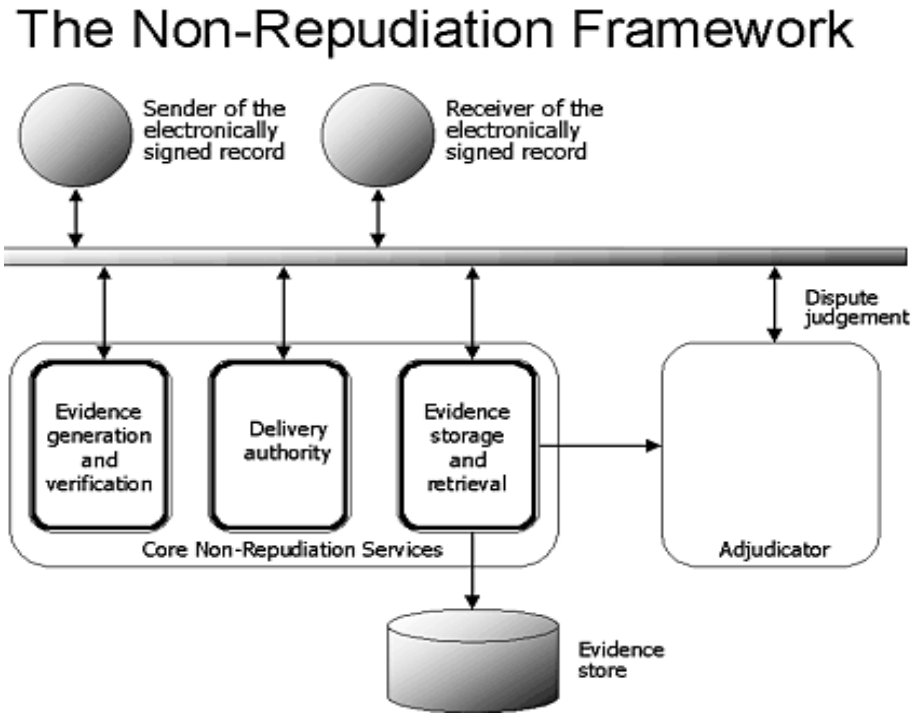


2.8. ỨNG DỤNG MÃ MẬT



2.9. ỨNG DỤNG XÁC THỰC, CHỐNG CHỐI BỎ





Ứng dụng xác thực của hệ thống chứng thực số

Ứng dụng chống chối bỏ của hệ thống chứng thực số

2.10. ĐẶC ĐIỂM CỦA CHỮ KÝ SỐ

- **Khái niệm CKS**: Chữ ký số là thông tin (Dữ liệu) được gắn kèm với tài liệu (văn bản, âm thanh, hình ảnh) sử dụng các thuật toán mật mã nhằm xác định người ký dữ liệu đó.

- **Mục đích của chữ ký số**:
  - Xác định người ký
  (++ Nguồn gốc tài liệu,
  ++ Ý định cá nhân trên tài liệu đó).
  - Xác định tính toàn vẹn của tài liệu

  Bản chất: chữ ký số là kết quả của một lược đồ toán học với đầu vào là dữ liệu cần ký, được tóm lược thông qua hàm băm và mã mật hóa dữ liệu đã tóm lược.
- **Kỹ thuật**: Chữ ký số được tạo và kiểm tra bằng các thuật toán mật mã.

2.10. ĐẶC ĐIỂM CỦA CHỮ KÝ SỐ

MỘT SỐ ĐIỂM KHÁC BIỆT GIỮA CHỮ KÝ SỐ VÀ CHỮ KÝ TAY

Khác biệt	Chữ ký tay	Chữ ký số
Mối quan hệ của chữ ký với người ký	Có mối liên hệ sinh học với cá nhân người ký.	Phụ thuộc vào nhà cung cấp dịch vụ chữ ký số.
Thực hiện ký và kiểm tra chữ ký	Ký bằng tay và kiểm tra chữ ký bằng mắt	Thông qua phần mềm máy tính
Chữ ký ở các tài liệu khác nhau	Gần giống nhau và không phụ thuộc vào tài liệu và thời điểm ký	Khác nhau và phụ thuộc vào từng tài liệu ký và thời điểm ký

2.10. ĐẶC ĐIỂM CỦA CHỮ KÝ SỐ

ƯU ĐIỂM CỦA CHỮ KÝ SỐ

Ưu điểm	Chữ ký tay	Chữ ký số
Việc giả mạo chữ ký	Vẫn có thể diễn ra trong thực tế.	Hầu như không thực hiện được (trừ trường hợp bị lộ khóa riêng hoặc bị lợi dụng).
Kỹ thuật phát hiện sự giả mạo chữ ký	Kiểm tra bằng mắt, phụ thuộc vào kỹ năng của người kiểm tra và cần một khoảng thời gian.	Kiểm tra bằng phần mềm, có kết quả tức thời và như nhau với bất kỳ ai kiểm tra.
Đảm bảo tính toàn vẹn tài liệu	Yếu (khả năng phát hiện sửa đổi tài liệu phụ thuộc vào từng cá nhân)	Mạnh (Dễ dàng và nhanh chóng phát hiện được tài liệu đã bị sửa đổi)

2.10. ĐẶC ĐIỂM CỦA CHỮ KÝ SỐ

NHƯỢC ĐIỂM CỦA CHỮ KÝ SỐ

Nhược điểm	Chữ ký tay	Chữ ký số
Thời hạn kiểm tra chữ ký	Gần như không có giới hạn.	Có thời hạn nhất định (thiết bị xử lý, kỹ thuật mật mã lạc hậu, chứng thư số hết hạn)
Tính đơn giản	Đơn giản khi thực hiện (ký và kiểm tra) và dễ chứng minh, dễ hiểu với bên thứ ba (quan tòa, thẩm phán, trọng tài…)	Rất phức tạp, khó khi chứng minh và khó hiểu với bên thứ ba (liên quan đến toán học, hệ điều hành, giao thức, xử lý đường dẫn chứng thực, chính sách…).

3. TRIỂN KHAI HỆ THỐNG CTS TRONG CQNN

3.1. MÔ HÌNH HỆ THỐNG CTS VIỆT NAM

3.2. HÀNH LANG PHÁP LÝ

3.3. CÁC DỊCH VỤ CUNG CẤP

3.4. CÁC SẢN PHẨM ỨNG DỤNG

3.5. KẾT QUẢ TRIỂN KHAI TẠI CÁC CQNN

3.6. KẾT QUẢ TRIỂN KHAI CHO CPĐT

3.7. ỨNG DỤNG CHỮ KÝ SỐ TẠI VIỆN KSNN

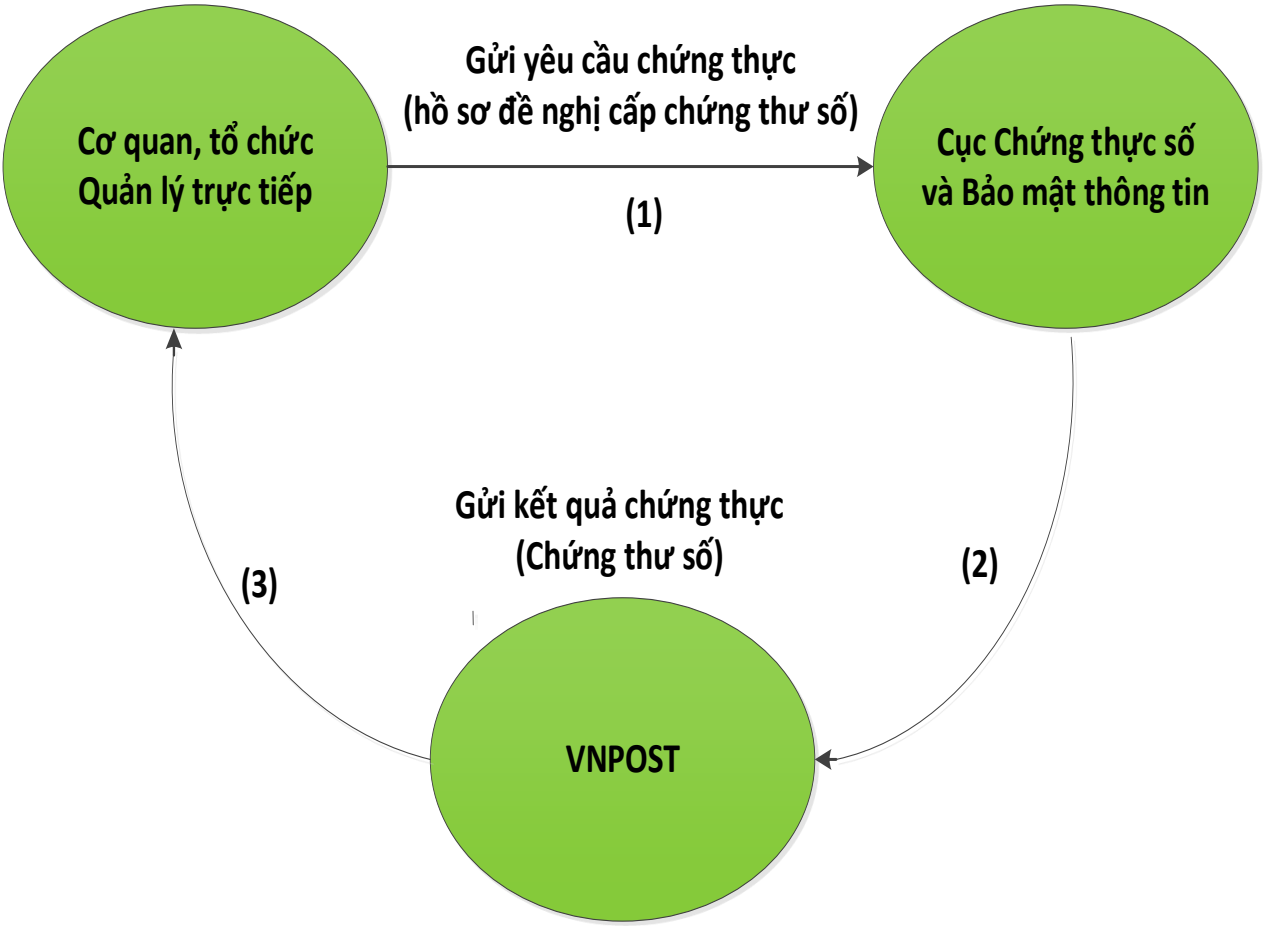
3.1. MÔ HÌNH HỆ THỐNG CHỨNG THỰC SỐ VN

3.2. HÀNH LANG PHÁP LÝ

- Luật giao dịch điện tử số 51/2005/QH11 quy định về giao dịch điện tử trong hoạt động của các cơ quan nhà nước, trong lĩnh vực dân sự, kinh doanh thương mại và các lĩnh vực khác.
- Nghị định số 130/2018/NĐ-CP ngày 27/9/2018 Quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số.
- Thông tư số 41/2017/TT-BTTTT của Bộ TTTT quy định sử dụng chữ ký số cho văn bản điện tử trong cơ quan nhà nước.
- Thông tư số 01/2019/TT-BNV quy định quy trình trao đổi, lưu trữ, xử lý tài liệu điện tử trong công tác văn thư, các chức năng cơ bản của Hệ thống quản lý tài liệu điện tử trong quá trình xử lý công việc của các cơ quan, tổ chức.
- Nghị quyết số 17/NQ-CP, ngày 07/3/2019 của Chính phủ Về một số nhiệm vụ, giải pháp trọng tâm phát triển CPĐT giai đoạn 2019 - 2020, định hướng đến 2025
- Quyết định số 28/2018/QĐ-TTg ngày 12/7/2018 của Thủ tướng CP về việc gửi, nhận văn bản điện tử giữa các cơ quan trong hệ thống hành chính nhà nước.
- Chỉ thị số 02/CT-TTg ngày 23/01/2019 của Thủ tướng CP về việc tăng cường sử dụng chữ ký số chuyên dùng chính phủ trong hoạt động của cơ quan nhà nước các cấp.

3.2. HÀNH LANG PHÁP LÝ

- Quy trình cung cấp chứng thư số theo Nghị định số 130/2018/NĐ-CP.



(1) Gửi yêu cầu chứng thực (hồ sơ đề nghị cấp chứng thư số): Cơ quan, tổ chức lập hồ sơ đề nghị cấp chứng thư số và gửi tới Cục CTS&BMTT.

(2) Cục CTS&BMTT giải quyết yêu cầu (tạo chứng thư số).

(3) Gửi kết quả chứng thực tới thuê bao: Thông qua dịch vụ trả kết quả thực hiện thủ tục hành chính của Bưu điện Việt Nam.

3.2. HÀNH LANG PHÁP LÝ

- Thông tư số 01/2019/TT-BNV quy định quy trình trao đổi, lưu trữ, xử lý tài liệu điện tử trong công tác văn thư, các chức năng cơ bản của Hệ thống quản lý tài liệu điện tử trong quá trình xử lý công việc của các cơ quan, tổ chức.
  - **Điều 12. Hình thức chữ ký số của người có thẩm quyền ký ban hành văn bản**
    - 1. Vị trí: tại vị trí ký của người có thẩm quyền ký ban hành văn bản trên văn bản giấy.
    - 2. Hình ảnh: chữ ký của người có thẩm quyền trên văn bản giấy, màu xanh, định dạng (.png).
  - **Điều 13. Hình thức chữ ký số của cơ quan, tổ chức ban hành văn bản**
    - 1. Vị trí: trùm lên khoảng 1/3 chữ ký của người có thẩm quyền về phía bên trái.
    - 2. Hình ảnh: dấu của cơ quan, tổ chức ban hành văn bản, màu đỏ, kích thước bằng kích thước thực tế của dấu, định dạng (.png).
    - 3. Thông tin: Tên cơ quan, tổ chức, thời gian ký (ngày, tháng, năm; giờ, phút, giây; múi giờ Việt Nam theo Tiêu chuẩn ISO 8601).

3.3. CÁC DỊCH VỤ CUNG CẤP

Dịch vụ chứng thực chữ ký số

- Cấp mới, gia hạn, tạm dừng/khôi phục, thu hồi chứng thư số.
  - Chứng thư số cho cá nhân (công chức).
  - Chứng thư số cho tổ chức (cơ quan).
  - Chứng thư số SSL cho dịch vụ, máy chủ (Web, VPN, Mail)…

Dịch vụ khẳng định tính hợp lệ chứng thư số (trực tuyến)

- Kiểm tra tính hợp lệ và tin cậy của chứng thư số: hợp lệ và tin cậy cho các giao dịch trên mạng: LDAP, CRL, OCSP.

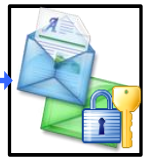
Dịch vụ cấp dấu thời gian (trực tuyến)

- Cung cấp dấu thời gian cho các giao dịch: TSA

3.4. CÁC SẢN PHẨM ỨNG DỤNG

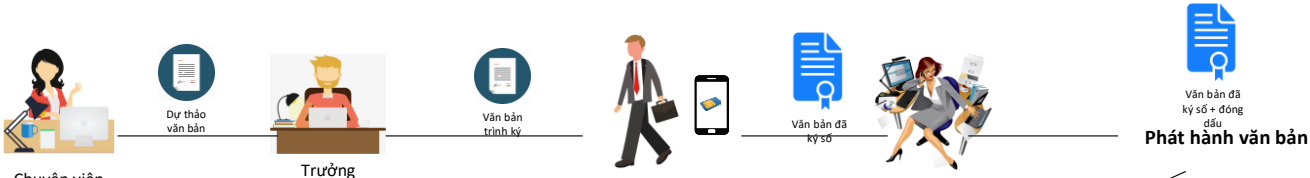
Ký số, xác thực tài liệu PDF

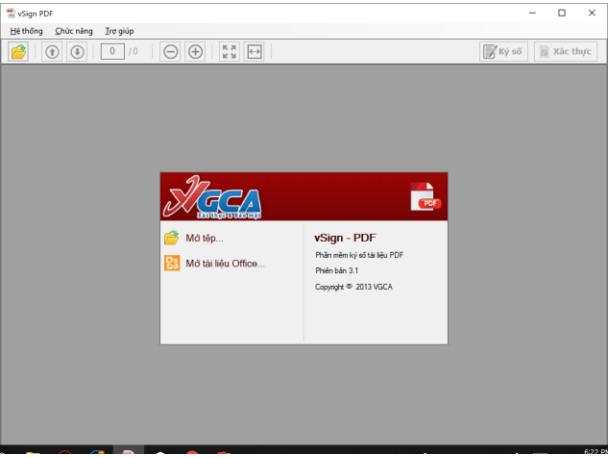
Ký số, xác thực tệp dữ liệu (định dạng bất kỳ)



Ký số, xác thực mật thư điện tử thông qua vùng nhớ đệm

- Ký số Desktop
- Ký số Web based
- Ký số trên mobile

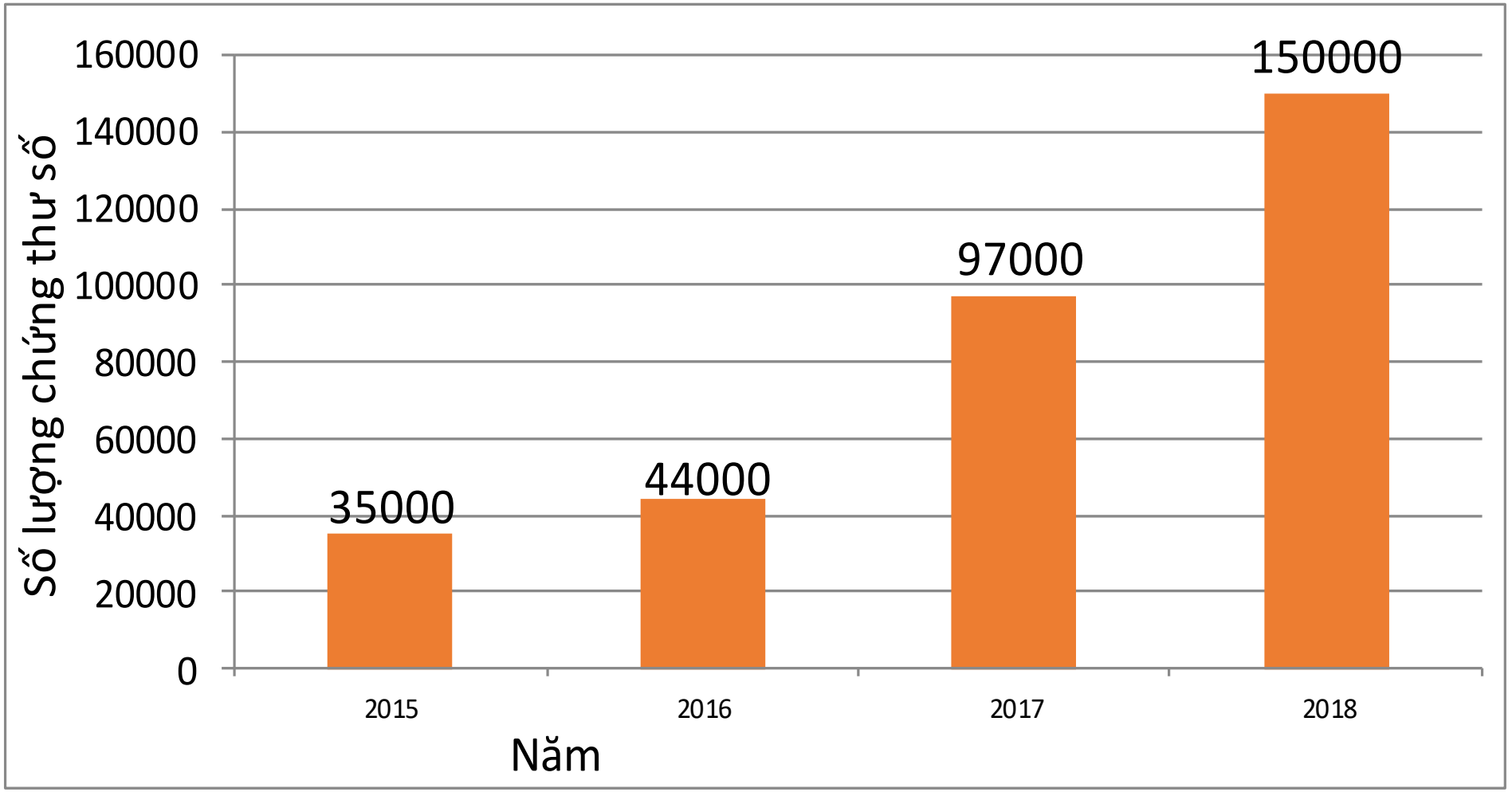




3.5. KẾT QUẢ TRIỂN KHAI TẠI CÁC CQNN

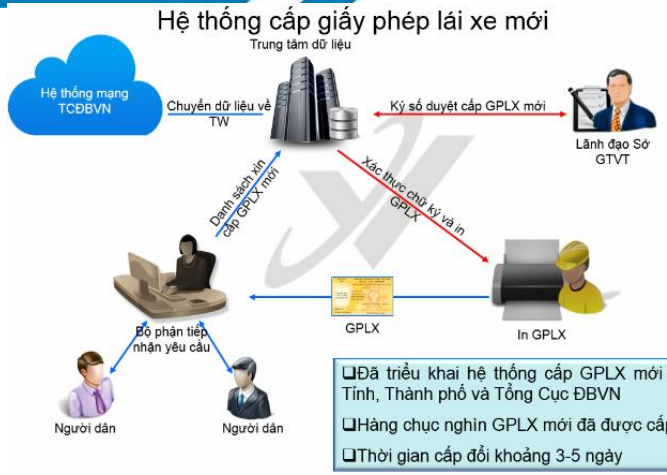
Cung cấp chứng thư số

Các bộ và cơ quan ngang bộ đã sử dụng: 28/32.
Các tỉnh/thành phố đã sử dụng: 49/63



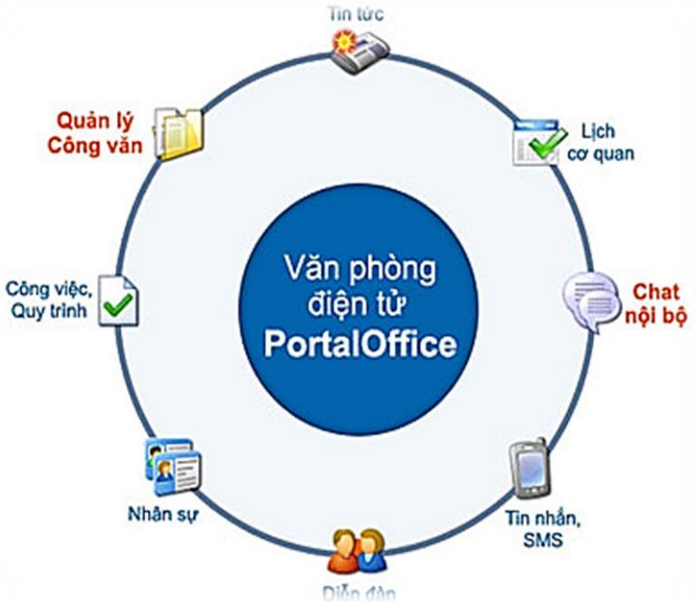
3.5. KẾT QUẢ TRIỂN KHAI TẠI CÁC CQNN

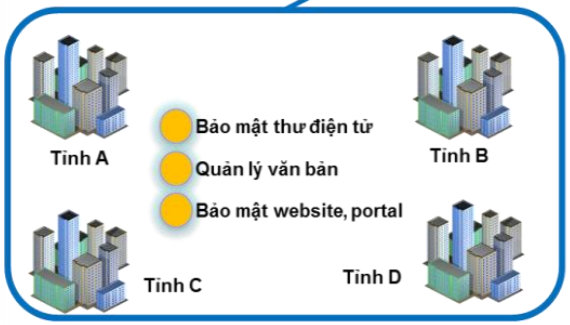
Tích hợp chữ ký số vào một số ứng dụng tại một số cơ quan Nhà nước

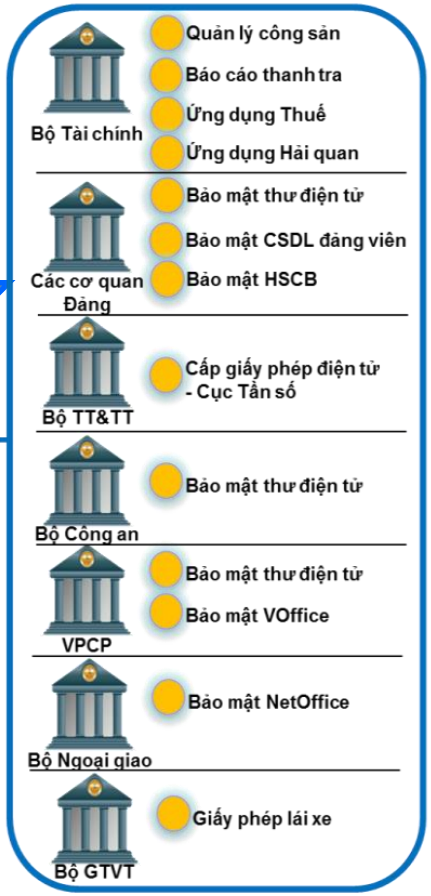


- Đã triển khai hệ thống cấp GPLX mới cho các Tỉnh, Thành phố và Tổng Cục ĐBVN
- Hàng chục nghìn GPLX mới đã được cấp, đổi
- Thời gian cấp đổi khoảng 3-5 ngày

- Cấp phát quản lý chứng thư số
- Dịch vụ chứng thực CKS
- Bộ công cụ ký số GCA-01
- Mobile PKI
- ePastport, e-Driver License, eID,...







3.6. KẾT QUẢ TRIỂN KHAI CHO CPĐT

HỆ THỐNG QUẢN LÝ VĂN BẢN VÀ ĐIỀU HÀNH

CỔNG DỊCH VỤ CÔNG QUỐC GIA

HỆ THỐNG THÔNG TIN BÁO CÁO QUỐC GIA

HỆ THỐNG THAM VẤN CHÍNH SÁCH (E-CONSULTATION)

HỆ THỐNG THÔNG TIN PHỤC VỤ HỌP VÀ XỬ LÝ CÔNG VIỆC CỦA CHÍNH PHỦ (E-CABINET)

CÁC HỆ THỐNG THÔNG TIN KHÁC ...

3.7. ỨNG DỤNG CHỨNG THƯ SỐ TẠI TTXVN

- Mục tiêu:
  - Xác thực người dùng đăng nhập vào hệ thống thông tin
  - Ký số vào văn bản điện tử.
  - Bảo mật đường truyền (VPN).
- Các ứng dụng:
  - Hệ thống xác thực tập trung.
  - Dịch vụ công BHXH, KBNN, Thuế.
  - Trao đổi văn bản hành chính Trục liên thông văn bản quốc gia.
  - Hệ thống thông tin nội bộ của TTVXN.
- Tổ chức thực hiện:
  - Đăng ký chứng thư số: (nghị định 130/2018/NĐ-CP).
  - Tập huấn hướng dẫn người dùng sử dụng phần mềm ký số.
  - Tích hợp chứng thư số vào phần mềm nghiệp vụ của TTXVN.

4. TÓM TẮT

- Ứng dụng CNTT trong các CQNN phát triển mạnh, kéo theo các vấn đề gây mất an toàn thông tin. Giải pháp tốt nhất hiện nay là ứng dụng hạ tầng khóa công khai (PKI) để đảm bảo an toàn cho các giao dịch điện tử.
- Hệ thống chứng thực số chuyên dùng Chính phủ, với 4 ứng dụng cơ bản: ký số, mã mật, xác thực, chống chối bỏ, đã cung cấp nhiều sản phẩm ứng dụng hiệu quả đảm bảo an toàn cho việc trao đổi thông tin trong các cơ quan Đảng, Nhà nước và phát triển Chính phủ điện tử.
- Triển khai, ứng dụng hệ thống chứng thực số tại Thông tấn xã Việt Nam sẽ thúc đẩy việc ứng dụng CNTT (chữ ký số) nâng cao tính xác thực, bảo mật, an toàn cho việc trao đổi thông tin trong các cơ quan thuộc TTXVN và với các tổ chức cá nhân có liên quan.

5. THẢO LUẬN

TRÂN TRỌNG

CẢM ƠN