CÔNG TÁC ĐẢM BẢO AN TOÀN, BẢO MẬT THÔNG TIN TRÊN MẠNG CNTT CÁC CƠ QUAN ĐẢNG VÀ NHÀ NƯỚC CỦA NGÀNH CƠ YẾU VIỆT NAM

Người trình bày: Nguyễn Hữu Hùng

Phó cục trưởng Cục Quản lý Kỹ thuật Nghiệp vụ Mật mã

BAN CƠ YẾU CHÍNH PHỦ

NỘI DUNG

I. MỘT SỐ NGUY CƠ ĐỐI VỚI AN TOÀN, BẢO MẬT THÔNG TIN TRONG CƠ QUAN ĐẢNG VÀ NHÀ NƯỚC

II. NHIỆM VỤ CỦA NGÀNH CƠ YẾU TRONG ĐẢM BẢO AN TOÀN VÀ BẢO MẬT THÔNG TIN

III. MỘT SỐ KẾT QUẢ TRIỂN KHAI

IV. KẾT LUẬN

I. MỘT SỐ NGUY CƠ ĐỐI VỚI AN TOÀN, BẢO MẬT THÔNG TIN TRÊN MẠNG CNTT CƠ QUAN ĐẢNG VÀ NHÀ NƯỚC

I. Một số nguy cơ đối với an toàn, bảo mật thông tin trên mạng CNTT cơ quan Đảng và Nhà nước

Tính bí mật của dữ liệu: dữ liệu có thể bị đọc trộm, nghe lén một cách trái phép…

Tính xác thực của dữ liệu, của các đối tượng giao dịch: dữ liệu có thể bị giả mạo, các đối tượng tham gia giao dịch bị mạo danh,…

Tính toàn vẹn của dữ liệu: dữ liệu bị sửa đổi trái phép trong giao dịch

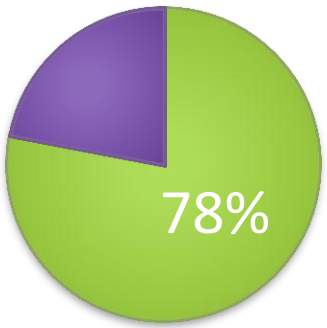
Tính chống chối bỏ: chối bỏ giao dịch, chối bỏ hành động gửi dữ liệu, ký dữ liệu, sửa dữ liệu, thời gian…

I.1. Nguy cơ qua website

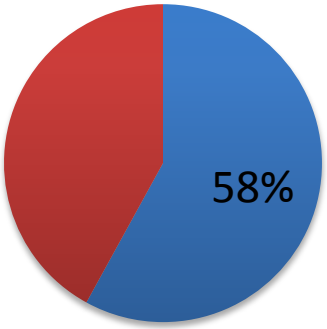
- Theo khảo sát của VNCERT năm 2012, 54% cơ quan Nhà nước không ghi nhận hành vi tấn công. Điều này đồng nghĩa với việc quá nửa các website ở Việt Nam dù "xây nhà" đã trang bị "khóa" song kẻ trộm vẫn có thể đột nhập mà chủ nhà không hề hay biết.
- Bên cạnh đó, 64% cơ quan Nhà nước không ước lượng được tổn thất tài chính khi bị tấn công

❑ Lựa chọn ngẫu nhiên 100 website (.gov.vn):

78 website có điểm yếu bảo mật ở mực độ "Nghiêm trọng" và "Cao"



58 website có điểm yếu bảo mật ở mực độ "Nghiêm trọng"



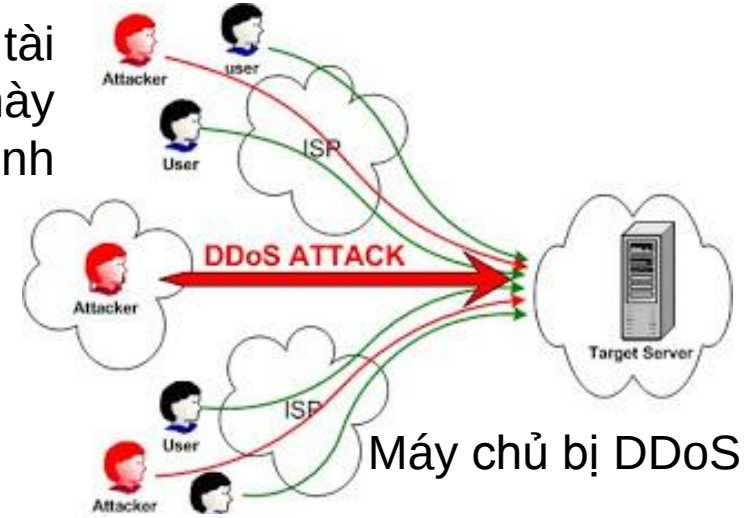
Nguồn: VNISA

I.2. Tấn công DDOS vào các báo điện tử

- DoS/DDoS là hình thức tấn công gây tê liệt tài nguyên mạng của nạn nhân làm cho tài nguyên này không thể phục vụ được cho người dùng bình thường.
- Các báo điện tử: Dân trí, VietNamNet, Tuổi trẻ

No.	Time	Source	Destination	Protocol	Length	Info
4	2013-07-08 19:10:56.999153	113.170.122.172	123.30.128.27	HTTP	596	GET /tin-tuc/ HTTP/1.1
12	2013-07-08 19:10:56.999591	192.157.56.179	123.30.128.27	HTTP	610	GET /tin-tuc/ HTTP/1.1
13	2013-07-08 19:10:56.999595	58.186.220.14	123.30.128.27	HTTP	604	GET /tin-tuc/ HTTP/1.1
19	2013-07-08 19:10:56.999799	58.186.95.176	123.30.128.27	HTTP	609	GET /tin-tuc/ HTTP/1.1
24	2013-07-08 19:10:56.999203	123.20.58.251	123.30.128.27	HTTP	609	GET /tin-tuc/ HTTP/1.1
25	2013-07-08 19:10:56.999208	113.167.122.83	123.30.128.27	HTTP	520	GET / HTTP/1.1
29	2013-07-08 19:10:56.999511	222.252.247.237	123.30.128.27	HTTP	527	GET / HTTP/1.1
35	2013-07-08 19:10:56.999010	183.81.16.82	123.30.128.27	HTTP	526	GET / HTTP/1.1
40	2013-07-08 19:10:56.999373	113.23.8.174	123.30.128.27	HTTP	604	GET /tin-tuc/ HTTP/1.1
42	2013-07-08 19:10:56.999465	50.117.80.108	123.30.128.27	HTTP	533	GET / HTTP/1.1
48	2013-07-08 19:10:56.999856	113.23.66.159	123.30.128.27	HTTP	520	GET / HTTP/1.1
56	2013-07-08 19:10:56.999165	222.254.99.242	123.30.128.27	HTTP	519	GET / HTTP/1.1
59	2013-07-08 19:10:56.999525	115.76.17.222	123.30.128.27	HTTP	527	GET / HTTP/1.1
62	2013-07-08 19:10:56.998987	113.162.127.255	123.30.128.27	HTTP	519	GET / HTTP/1.1
71	2013-07-08 19:10:56.999564	113.168.55.31	123.30.128.27	HTTP	587	GET /tin-tuc/ HTTP/1.1
73	2013-07-08 19:10:56.999616	118.68.203.42	123.30.128.27	HTTP	606	GET /tin-tuc/ HTTP/1.1
74	2013-07-08 19:10:56.999619	113.169.118.161	123.30.128.27	HTTP	591	GET /tin-tuc/ HTTP/1.1
77	2013-07-08 19:10:56.999694	117.3.140.1	123.30.128.27	HTTP	599	GET /tin-tuc/ HTTP/1.1
81	2013-07-08 19:10:56.999882	42.113.20.205	123.30.128.27	HTTP	526	GET / HTTP/1.1
88	2013-07-08 19:10:56.999055	203.205.25.98	123.30.128.27	HTTP	595	GET /tin-tuc/ HTTP/1.1
91	2013-07-08 19:10:56.999204	50.117.80.60	123.30.128.27	HTTP	596	GET /tin-tuc/ HTTP/1.1
97	2013-07-08 19:10:56.999058	115.73.44.96	123.30.128.27	HTTP	597	GET /tin-tuc/ HTTP/1.1
111	2013-07-08 19:10:56.999056	1.54.226.213	123.30.128.27	HTTP	519	GET / HTTP/1.1
119	2013-07-08 19:10:56.999625	27.74.147.219	123.30.128.27	HTTP	527	GET / HTTP/1.1
124	2013-07-08 19:10:56.999767	113.166.248.15	123.30.128.27	HTTP	520	GET / HTTP/1.1
127	2013-07-08 19:10:56.999907	113.165.172.156	123.30.128.27	HTTP	594	GET /tin-tuc/ HTTP/1.1
132	2013-07-08 19:10:57.000186	115.76.82.212	123.30.128.27	HTTP	584	GET /tin-tuc/ HTTP/1.1
143	2013-07-08 19:10:57.000788	58.187.199.73	123.30.128.27	HTTP	519	GET / HTTP/1.1
149	2013-07-08 19:10:57.000237	58.186.20.211	123.30.128.27	HTTP	587	GET /tin-tuc/ HTTP/1.1

Danh sách các địa chỉ IP **Botnet: Ít nhất 14 nghìn máy**



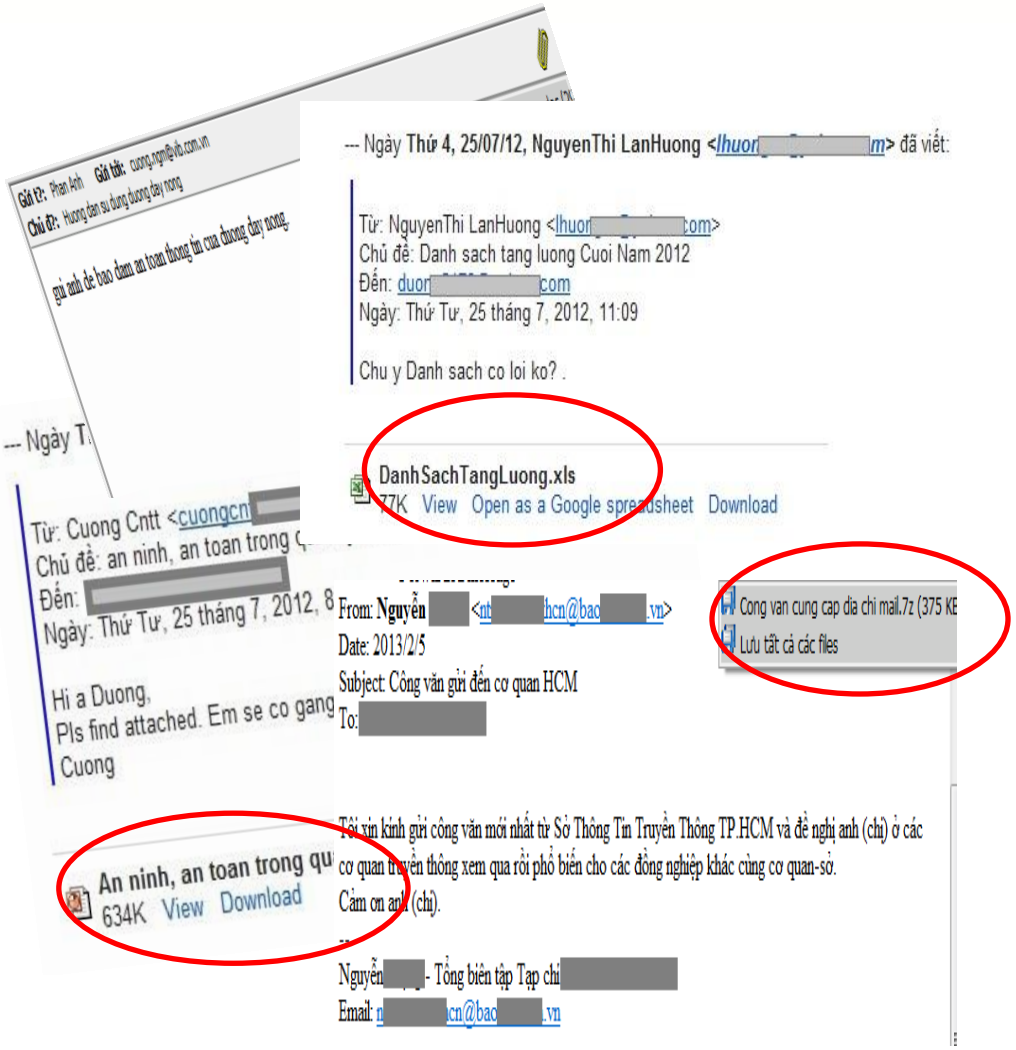
Máy chủ bị DDoS

Người dùng bị từ chối phục vụ

Mã độc: Có nhiều biến thể hàng ngày. Biến thể cuối cùng là ngày 25/7!!!

I.3. Nguy cơ qua hệ thống thư điện tử

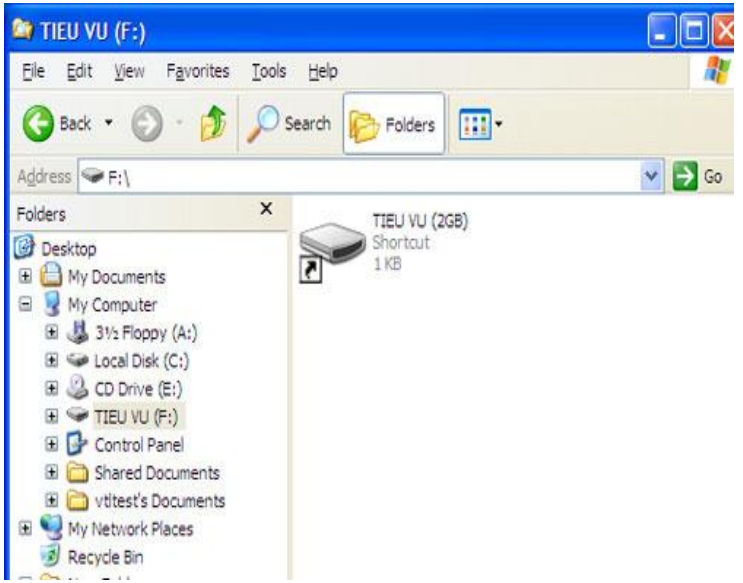
- Những mẫu virus mới thường giả mạo địa chỉ email của một cán bộ trong đơn vị để gửi file tài liệu cho các cán bộ khác với nội dung bằng tiếng Việt liên quan như tiền lương tháng, xin ý kiến, chương trình công tác... nhằm mục đích dụ tải về file đính kèm, từ đó sẽ khai thác các lỗ hổng của phần mềm Microsoft Office để thu thập thông tin, dữ liệu trong máy tính và gửi về các máy chủ ở nước ngoài, trong đó nhiều máy chủ có địa chỉ ở Trung Quốc
- Tin tặc thường tìm hiểu kỹ tên tuổi, chức vụ của những người trong cơ quan nhà nước trước khi tiến hành phát tán mã độc qua email. Những mẫu virus này vì chỉ dành cho đối tượng xác định nên thường "qua mặt" các phần mềm diệt virus. "Chiến dịch phát tán mã độc đánh cắp thông tin này xuất hiện từ tháng 7/2012 và đối tượng nhắm đến là các Bộ, ngành quan trọng của Việt Nam"



I.4. Nguy cơ lộ lọt thông tin qua thiết bị nhớ USB

Lộ lọt dữ liệu trong các cơ quan nhà nước qua thiết bị nhớ USB

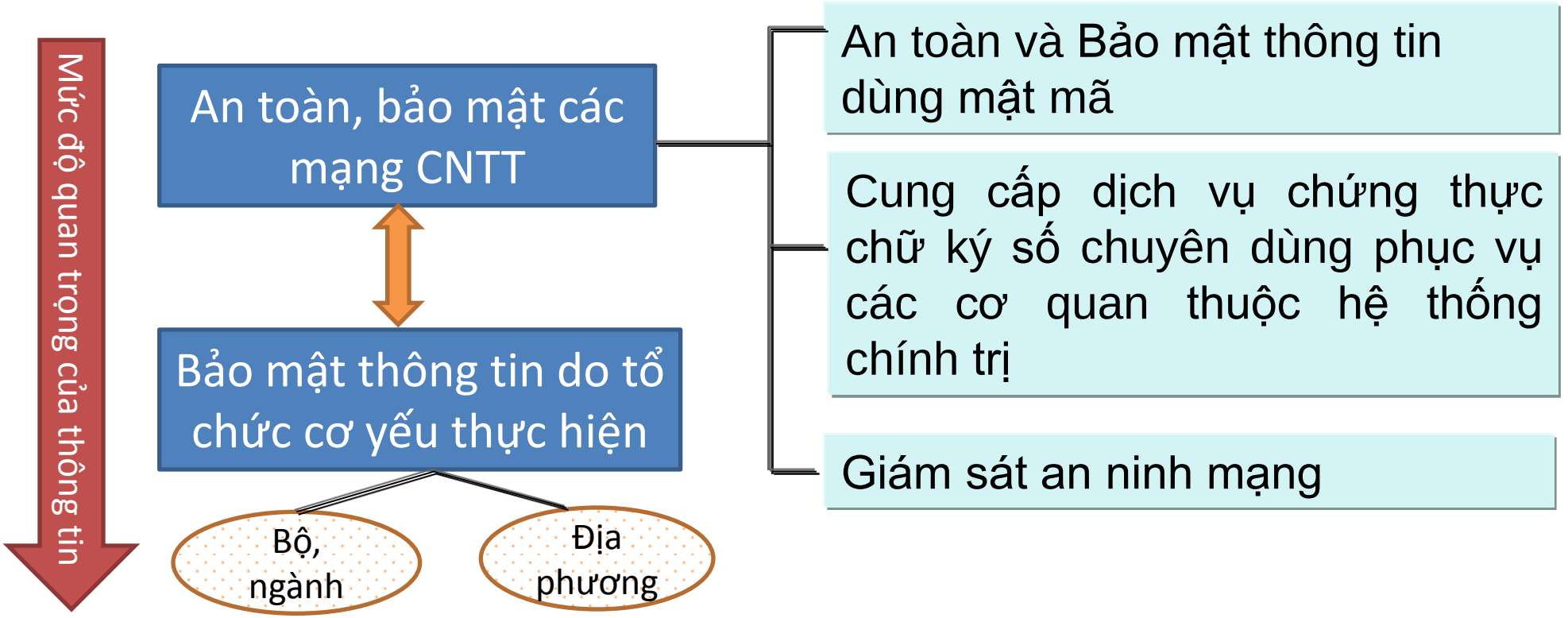
- Năm 2011, cơ quan chức năng Bộ Công an đã phát hiện loại malware, trojan chuyên lấy cắp thông tin mật lây nhiễm qua USB hoặc thâm nhập qua cửa hậu (back door) vào máy tính, và tự động đánh cắp tất cả văn bản nhạy cảm lưu trong máy về địa chỉ bên ngoài (Trung Quốc). Đã có trường hợp lộ, lọt cả dự thảo văn kiện chỉ đạo của Trung ương hoặc dự thảo văn bản thỏa thuận của đoàn đàm phán quốc tế.
- *Tỷ lệ rất cao các thiết bị lưu trữ USB bán trên thị trường hiện nay có cài sẵn mã độc.*
- **Hiện nay 1 loại virus mới lây qua USB với tốc độ rất nhanh** - *W32.UsbFakeDrive,* Khi mở USB bị nhiễm virus, người sử dụng sẽ thấy một ổ đĩa nữa trong USB đó và phải mở tiếp ổ đĩa thứ hai này mới thấy được dữ liệu. Thực chất, ổ đĩa thứ hai chính là một shortcut chứa file virus. Khi người dùng mở dữ liệu cũng là lúc máy tính bị nhiễm mã độc từ USB -> dữ liệu có thể bị đánh cắp



II. NHIỆM VỤ CỦA NGÀNH CƠ YẾU TRONG ĐẢM BẢO AN TOÀN, BẢO MẬT THÔNG TIN

II. Nhiệm vụ ngành Cơ yếu trong đảm bảo an toàn, bảo mật thông tin

- Ngành Cơ yếu Việt Nam tổ chức thực hiện đảm bảo an toàn, bảo mật thông tin phục vụ sự lãnh đạo, chỉ đạo, điều hành của Đảng và Nhà nước thông qua hệ thống kỹ thuật mật mã do Cơ yếu trực tiếp sử dụng và cung cấp sản phẩm an toàn, bảo mật trên các mạng CNTT của các cơ quan Đảng và Nhà nước:



II.1. An toàn và Bảo mật thông tin dùng mật mã

❑ Luật Cơ yếu, số 05/2011/QH13 ngày 26/11/2011:

- Ban Cơ yếu Chính phủ là cơ quan mật mã quốc gia, quản lý chuyên ngành về cơ yếu, có trách nhiệm giúp Bộ trưởng Bộ Quốc phòng thực hiện nhiệm vụ quản lý nhà nước về cơ yếu.
- Thông tin bí mật nhà nước được truyền bằng các phương tiện thông tin, viễn thông phải được mã hóa bằng mật mã của cơ yếu.
- Thông tin bí mật nhà nước lưu giữ trong các phương tiện thiết bị điện tử, tin học và trên mạng viễn thông được mã hoá bằng mật mã của cơ yếu

❑ Nghị định số 64/2007/NĐ-CP ngày 10/04/2007 về Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước:

- Chủ trì xây dựng và đề xuất ban hành các văn bản quy phạm pháp luật về mật mã trong an toàn và bảo mật thông tin;
- Xây dựng và đề xuất các tiêu chuẩn và quy chuẩn kỹ thuật mật mã trong an toàn và bảo mật thông tin; Tổ chức kiểm định, đánh giá và cấp chứng nhận các sản phẩm mật mã trong hoạt động các cơ quan Nhà nước;
- Triển khai các hệ thống bảo vệ thông tin thuộc phạm vi bí mật nhà nước dùng mật mã

II.2. Triển khai hệ thống CA chuyên dùng CP

- Nghị định 26/2007/NĐ-CP ngày 15/2/2007 quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số.
- Chỉ thị 34/2008/CT-TTg ngày 3 tháng 12 năm 2008 về việc tăng cường sử dụng thư điện tử trong hoạt động các cơ quan Nhà nước.
- Quyết định số 48/2009/QĐ-TTg ngày 31/3/2009 của Thủ tướng Chính phủ về việc phê duyệt Kế hoạch ứng dụng công nghệ thông tin trong hoạt động của các cơ quan Nhà nước giai đoạn 2009-2011.
- Quyết định 1605/QĐ-TTg ngày 27/8/2010 của Thủ tướng Chính phủ về việc phê duyệt chương trình quốc gia về ứng dụng CNTT giai đoạn 2011-2015.
- Chỉ thị số 897/CT-TTg ngày 10/6/2011 của Thủ tướng Chính phủ về việc tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số.
- Chỉ thị số 15/CT-TTg ngày 22/5/2012 của Thủ tướng Chính phủ về tăng cường sử dụng văn bản điện tử trong hoạt động của cơ quan nhà nước.

II.3. Triển khai hệ thống giám sát an ninh mạng

- **Chỉ thị số 897/CT-TTg ngày 10/6/2011 của Thủ tướng Chính phủ về việc tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số:**

- Chủ trì triển khai các hệ thống bảo mật, an toàn thông tin dùng mật mã cho các cơ quan nhà nước. Đẩy mạnh hoạt động của hệ thống chứng thực điện tử chuyên dùng phục vụ cho các cơ quan thuộc hệ thống chính trị. Xây dựng các văn bản hướng dẫn triển khai chứng thực và áp dụng chữ ký số chuyên dùng cho các cơ quan thuộc hệ thống chính trị.
- Tăng cường công tác quản lý nhà nước về mật mã, thúc đẩy ứng dụng mật mã phục vụ phát triển kinh tế - xã hội cho các hoạt động ứng dụng công nghệ thông tin và dịch vụ công nghệ thông tin trên mạng; hoàn thiện và hiện đại hóa hạ tầng cơ sở mật mã quốc gia.
- ***Chủ trì, phối hợp với các cơ quan liên quan triển khai hệ thống giám sát an toàn thông tin trên mạng công nghệ thông tin trọng yếu của các cơ quan Đảng, Chính phủ. Nghiên cứu, đề xuất ban hành các tiêu chuẩn, quy chuẩn kỹ thuật cho các sản phẩm mật mã. Đẩy mạnh hoạt động kiểm định, đánh giá sản phẩm mật mã.***

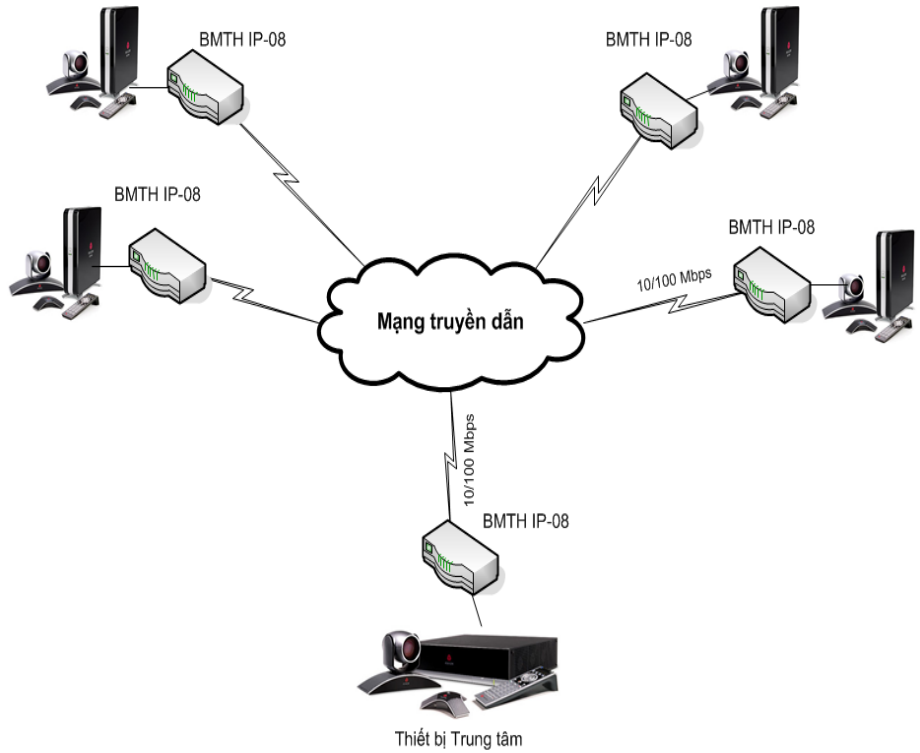
III. MỘT SỐ KẾT QUẢ TRIỂN KHAI

III.1. Nghiên cứu, triển khai sản phẩm bảo mật trên mạng CNTT

❑ **Bảo mật hội nghị truyền hình, mạng truyền số liệu:**

- Bảo mật hệ thống HNTH.
- Chế độ làm việc điểm – điểm và điểm – đa điểm
- Được thiết kế bằng phần cứng, sử dụng chip FPGA Spartan3E, dùng để bảo mật các gói IP trong mạng LAN, WAN hay mạng Internet.
- Tốc độ mã hóa/giải mã tối đa đo được 80 Mbps
- Cấu hình hoàn toàn tự động khi bật nguồn

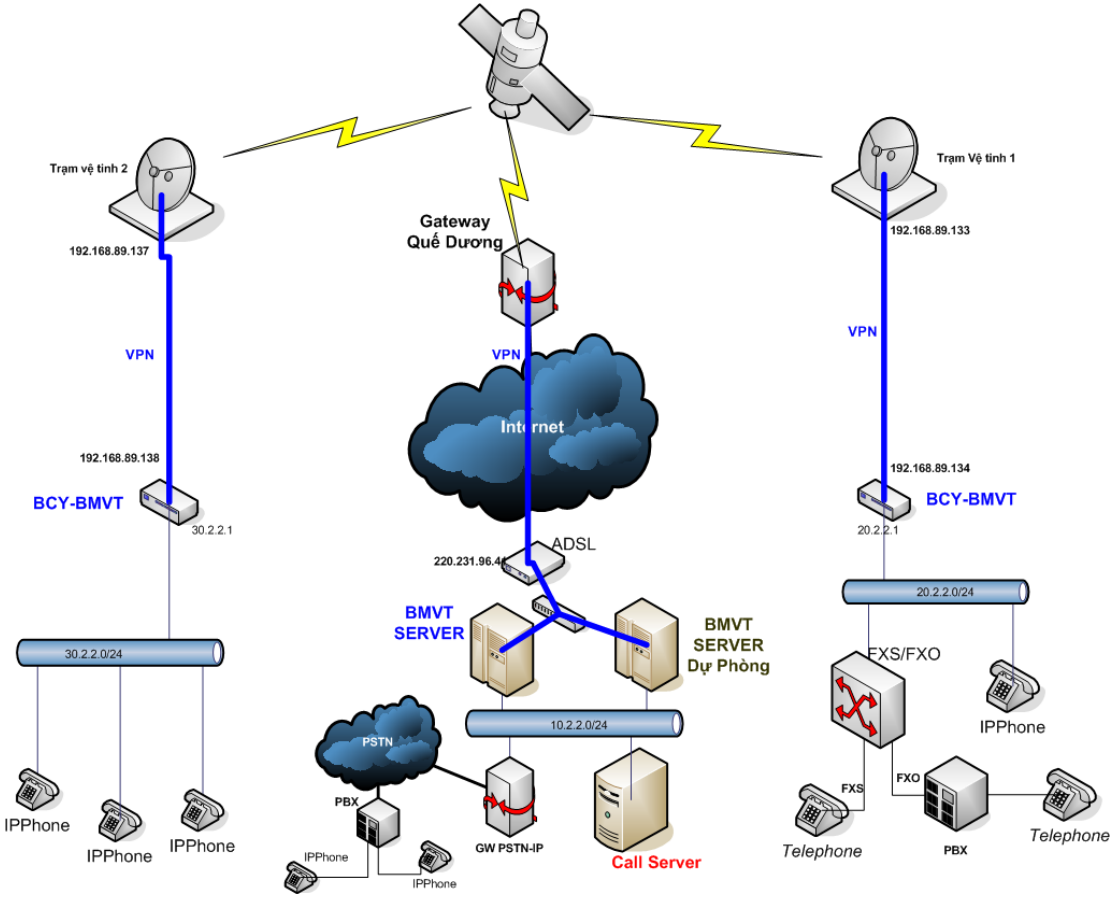
➢ Sử dụng mật mã của ngành cơ yếu



III.1. Nghiên cứu, triển khai sản phẩm bảo mật trên mạng CNTT (tiếp)

❑ **Bảo mật thông tin vệ tinh:**

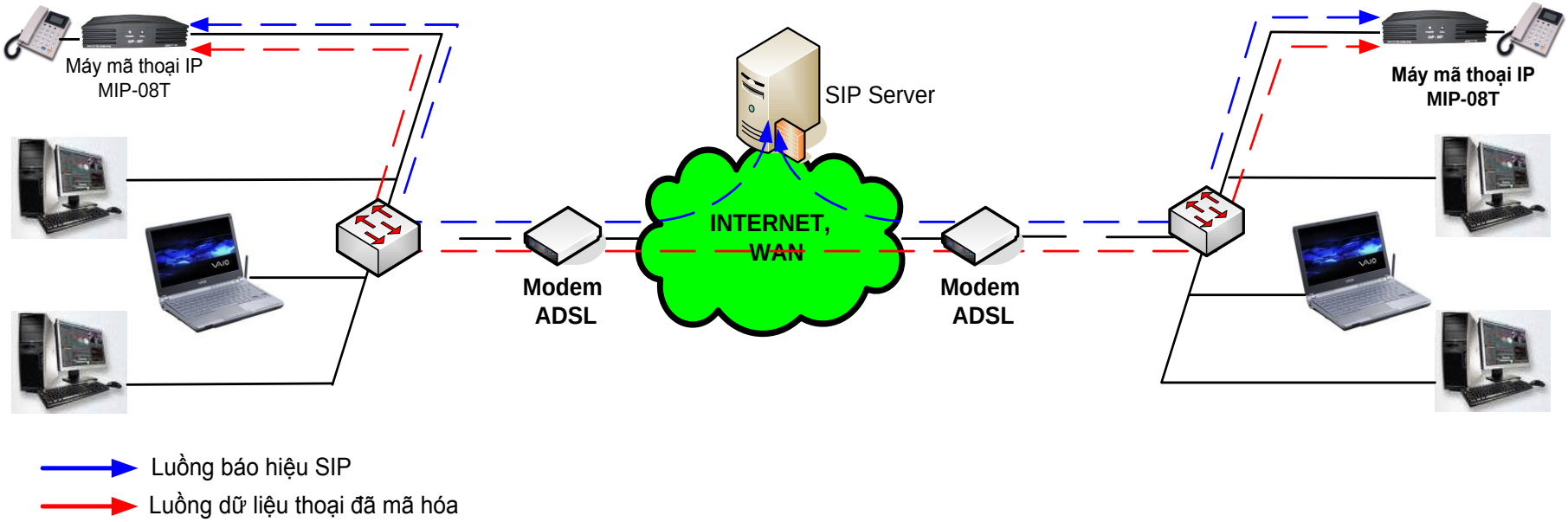
- Chức năng: tạo các kênh an toàn trên hệ thống liên lạc vệ tinh để bảo mật và xác thực dữ liệu trên đường truyền vệ tinh
- Có thể bảo vệ các thông tin như video, thoại (điện thoại vệ tinh)
- Sử dụng mật mã của ngành cơ yếu



III.1. Nghiên cứu, triển khai sản phẩm bảo mật trên mạng CNTT (tiếp)

❑ Bảo mật tín hiệu thoại VoIP:

- Máy mã VoIP MIP-08T có tính năng bảo mật các gói tin IP giữa đầu cuối – đầu cuối trong mạng LAN, WAN, Internet và mạng Vệ Tinh.
- Có đầy đủ các tính năng cơ bản của một điện thoại IP thông thường.



III.1. Nghiên cứu, triển khai sản phẩm bảo mật trên mạng CNTT (tiếp)

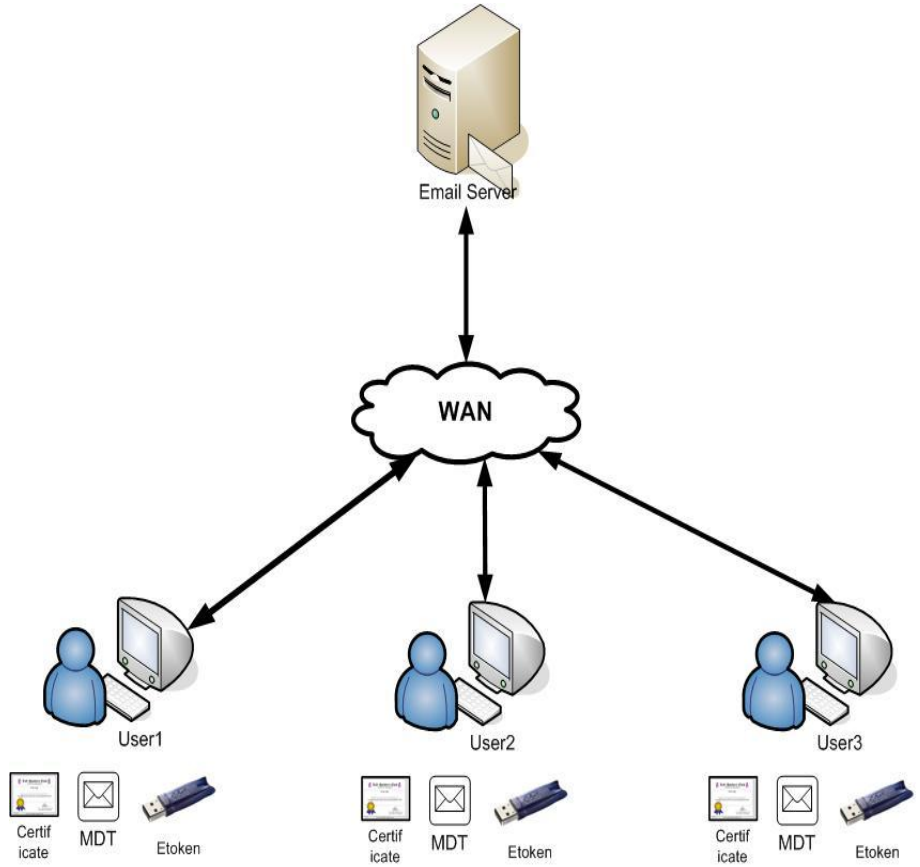
❑ **Bảo mật dữ liệu thoại trên điện thoại di động:**

- Hoạt động theo nguyên lý kỹ thuật số.
- Hoạt động trên mạng điện thoại GSM có hỗ trợ dịch vụ Data.
- Giao tiếp với điện thoại di động qua cổng Bluetooth.
- Nghe, nói thông qua tai nghe rời
- Tốc độ truyền 4800 hoặc 9600 bps

III.1. Nghiên cứu, triển khai sản phẩm bảo mật trên mạng CNTT (tiếp)

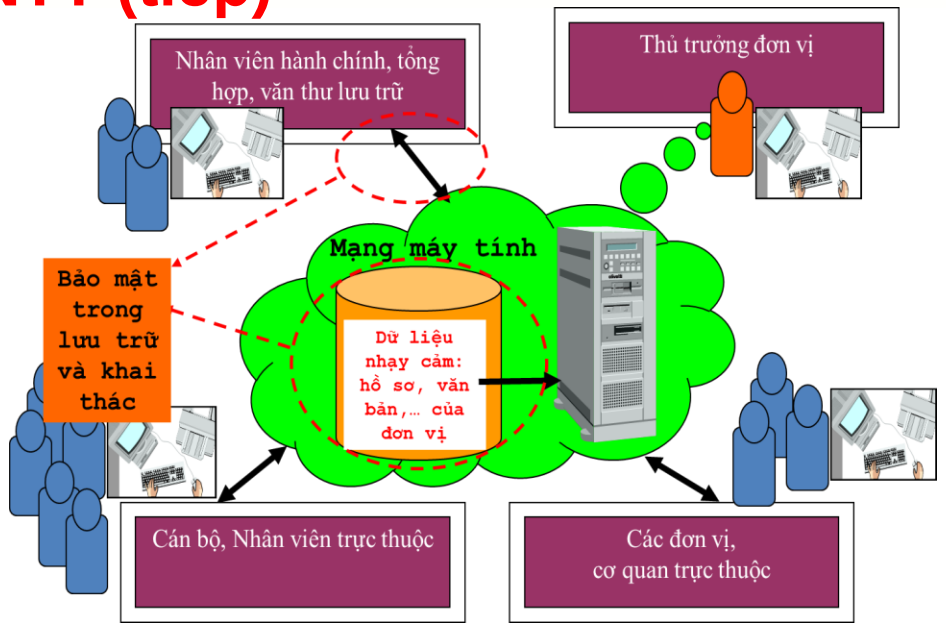
Bảo mật thư điện tử:

- Hệ thống thư điện tử mật giải quyết được:
  - Đảm bảo an toàn dữ liệu trên đường truyền từ nguồn đến đích.
  - Đảm bảo an toàn CSDL thư tại máy trạm - Mail Client.
  - Đảm bảo an toàn tại các Mail Server.
- Các hoạt động bảo mật xác thực thư điện tử dựa trên các dịch vụ chứng thực điện tử của hệ thống CA chuyên dùng Chính phủ
- Bên cạnh những vấn đề về kỹ thuật cần giải quyết thì các vấn đề như : Chính sách an toàn, môi trường vận hành và hệ thống quản lý an toàn cho hệ thống thư điện tử mật cũng cần phải được áp dụng



III.1. Nghiên cứu, triển khai sản phẩm bảo mật trên mạng CNTT (tiếp)

- **Bảo mật cơ sở dữ liệu:**
  - SQLEncrypt (Hệ quản trị CSDL SQL Server 2000, 2005, 2008)
  - OraEncypt (Hệ quản trị CSDL Oracle)
- **Bảo mật, xác thực web:**
  - Khôi phục dữ liệu công khai bị hacker sửa đổi hoặc xóa trái phép,
  - Bảo mật đối với dữ liệu nhạy cảm khi khai thác.
  - Bảo mật cho giao dịch điện tử có sử dụng công cụ web
  - Kiểm soát truy nhập dữ liệu web



III.1. Nghiên cứu, triển khai sản phẩm bảo mật trên mạng CNTT (tiếp)

- **Thiết bị nhớ an toàn (USB an toàn):**

- Dữ liệu lưu trữ trong các không gian bộ nhớ của thiết bị đều được mã hóa (không thể truy xuất dữ liệu khi gắn thẻ sang thiết bị đọc/ghi khác), việc xử lý dữ liệu (mã hóa, giải mã) đều được thực hiện trên thiết bị và trong suốt với người dùng.
- Thiết bị có cơ chế xác thực riêng, độc lập; với sự hỗ trợ của người dùng thông qua bàn phím gắn trên thiết bị, hoặc chương trình kèm theo.
- Thiết bị giao tiếp qua cổng USB (tương thích 1.1, 2.0, 3.0).
- Sử dụng chương trình riêng để thao tác với dữ liệu trong thiết bị. Không thể can thiệp được bằng các ứng dụng khác của HĐH.
- Có cơ chế tự xóa dữ liệu khi nhập sai mật khẩu một số lần quy định hoặc mở máy trái phép.
- **Chống được các virus tự động lây lan sang các thiết bị USB: Autorun, W32.UsbFakeDrive (chủng virus mới), chống sao chép dữ liệu bất hợp pháp**

Thiết bị (1) có bàn phím hỗ trợ

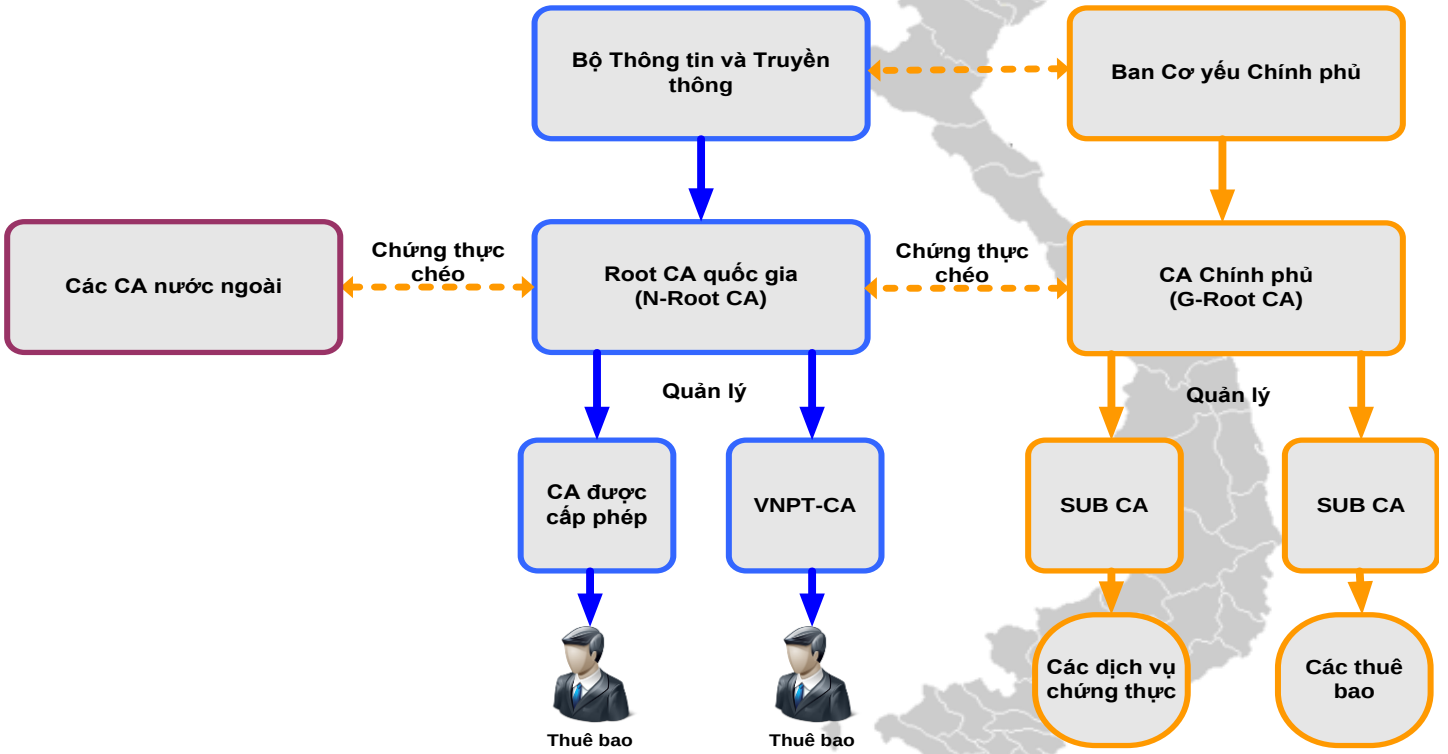
Thiết bị (2) không có bàn phím hỗ trợ

III.2. Hệ thống cung cấp dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ

Vấn đề an toàn	Phương pháp	Công nghệ bảo mật
Lộ lọt, đọc trộm	Bảo mật	Công nghệ mã hóa
Khó xác định danh tính	Xác thực	Công nghệ chữ ký số (Xác thực danh tính)
Sửa đổi, giả mạo	Đảm bảo toàn vẹn	Công nghệ chữ ký số (Xác thực thông điệp)
Chối bỏ hành động	Chống chối bỏ	Công nghệ chữ ký số (Xác thực thông điệp)

III.2. Hệ thống cung cấp dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ (tiếp)

Mô hình hệ thống CA quốc gia



- Giao dịch điện tử nội bộ cơ quan nhà nước và giữa các cơ quan nhà nước với nhau
- Các thông tin chỉ đạo, điều hành, tác nghiệp của cơ quan nhà nước các cấp

III.2. Hệ thống cung cấp dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ (tiếp)

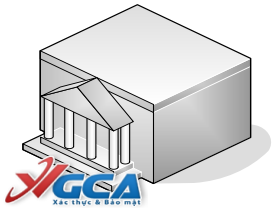
Quá trình phát triển

2002

Hạ tầng khóa công khai (PKI) đã sớm được Ban Cơ yếu Chính phủ nghiên cứu ứng dụng

2006

Triển khai thử nghiệm ứng dụng của chứng thư số, chữ ký số trên một số mạng công nghệ thông tin



2007

Thành lập Trung tâm chứng thực điện tử chuyên dùng Chính phủ theo Nghị định 26/2007/NĐ-CP

2010

Hệ thống đã được thiết lập và đưa vào sử dụng đồng bộ cả về hệ thống chính sách, quy trình, thủ tục, con người và hạ tầng kỹ thuật

2011, 2012

Tập trung nghiên cứu và xây dựng các giải pháp ứng dụng chữ ký số: bộ GCA-01, ký web, Mobile PKI, Sign/Verify Server tích hợp CKS vào các hệ thống thông tin của các cơ quan thuộc hệ thống chính trị

III.2. Hệ thống cung cấp dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ (tiếp)

Các dịch vụ chứng thực số

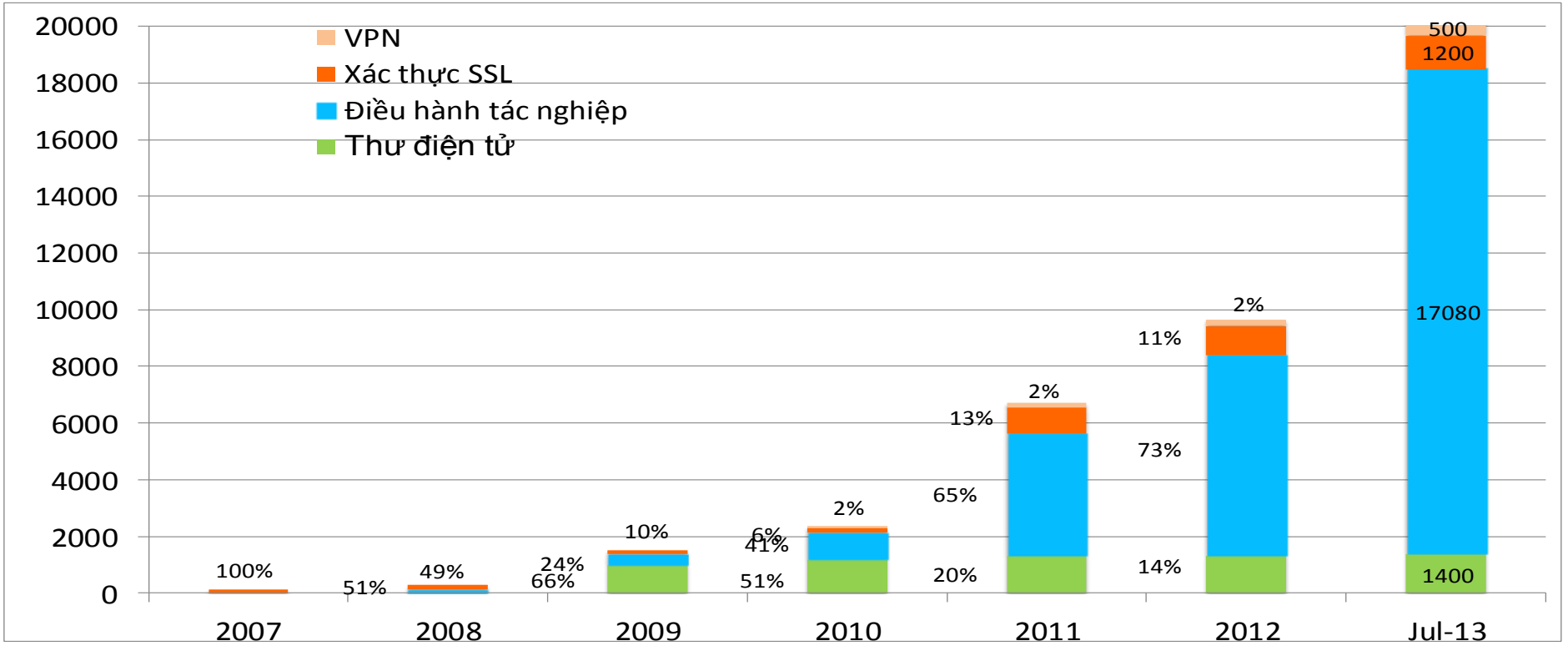
- Phân phối khóa an toàn cho các sản phẩm an toàn, bảo mật các mạn CNTT.
- Cung cấp dịch vụ xác thực, tin cậy:
  - Triển khai ứng dụng chữ ký số trong hệ thống thư điện tử, văn bản điện tử, hệ thống quản lý văn bản và hồ sơ công việc.
  - Ứng dụng cho các dịch vụ công mức 1, 2, 3, 4
- Cung cấp bộ công cụ PKI Tookit để tích hợp vào các hệ thống thông tin:
  - Ứng dụng Desktop
  - Ứng dụng Web

III.2. Hệ thống cung cấp dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ (tiếp)

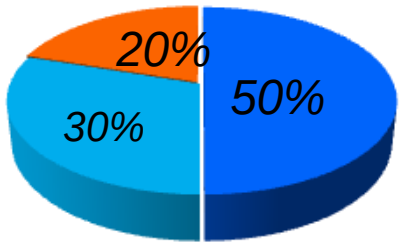
Ứng dụng CA trong Cơ quan Nhà nước:

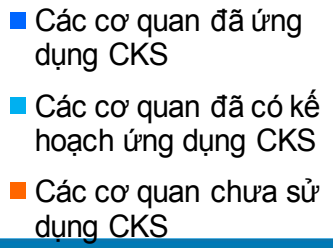
- Xác thực
  - Ký số/xác thực văn bản điện tử, thư điện tử
  - Ký số/xác thực dữ liệu trong phần mềm điều hành tác nghiệp
  - Xác thực định danh người sử dụng cho các hệ thống phần mềm, cổng thông tin điện tử, dịch vụ công
- Bảo mật
  - Mã hóa/Giải mã văn bản điện tử, thư điện tử
  - Thiết lập các kênh truyền dữ liệu mật cho phép người dùng làm việc từ xa (HTTPS, VPN).
  - Mã hóa/Giải mã dữ liệu gửi nhận trong các hệ thống phần mềm điều hành tác nghiệp.

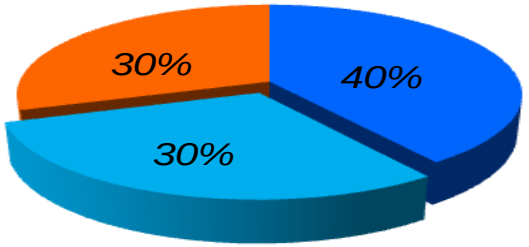
Tình hình ứng dụng chữ ký số tại các Bộ, ngành và địa phương



Trung ương







Địa phương

Kết quả kiểm tra, đánh giá tình hình ứng dụng chữ ký số trong cơ quan nhà nước theo chỉ thị 15/CT-TTg

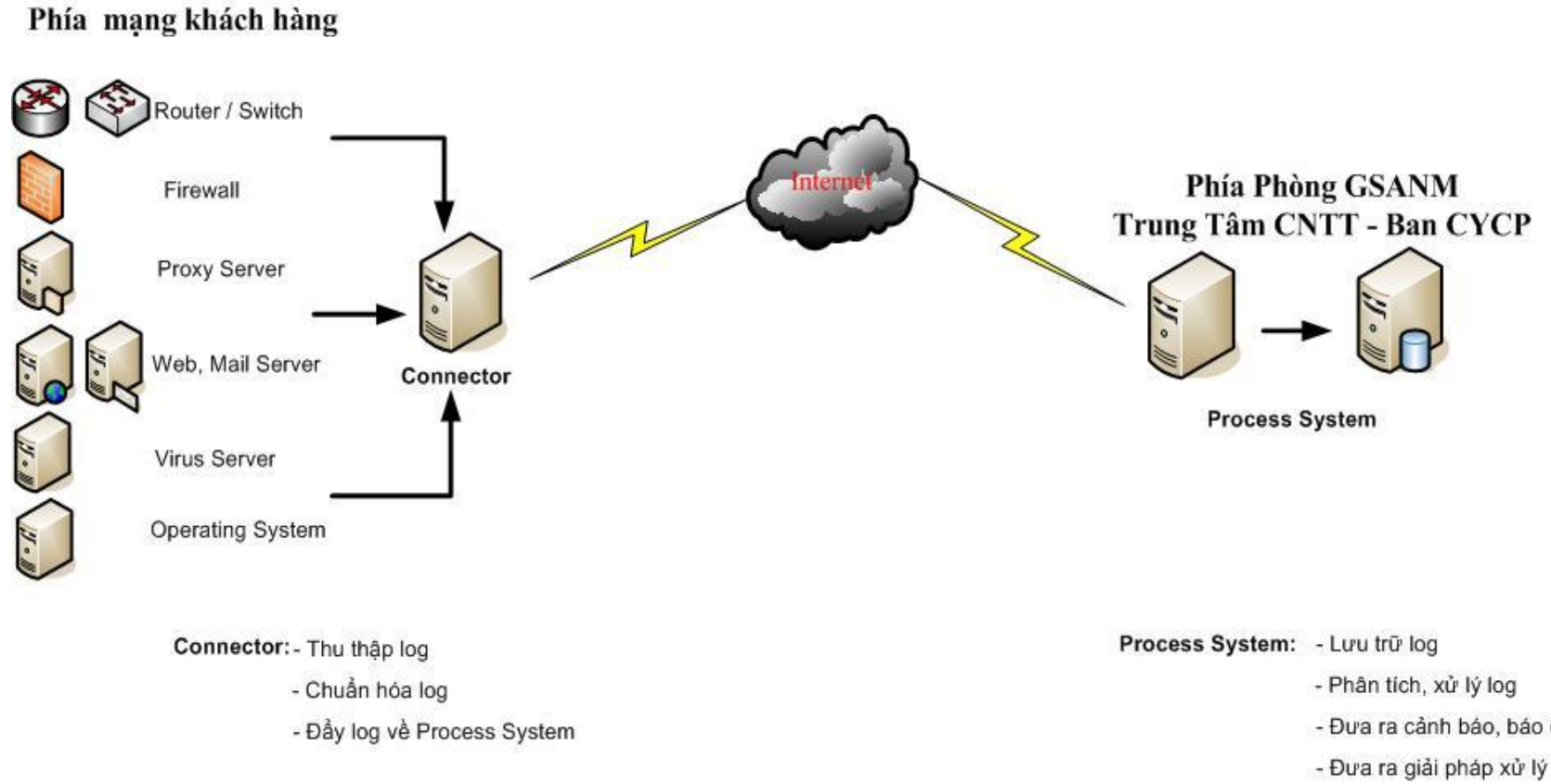
❑ Đoàn công tác liên ngành giữa Ban Cơ yếu Chính phủ và cơ quan chức năng của Bộ TT&TT thực hiện kiểm tra, đánh giá tại 12 đầu mối cơ quan nhà nước (04 Bộ, cơ quan ngang Bộ và 08 địa phương).

❑ **Kết quả:**

- Nhận thức về vai trò, tầm quan trọng của chữ ký số từ cấp lãnh đạo đến cán bộ, công chức được chuyển biến rõ rệt.
- Việc ứng dụng chứng thư số do Ban Cơ yếu Chính phủ cung cấp đã phát huy hiệu quả trong hoạt động quản lý, điều hành và tác nghiệp của các cơ quan nhà nước, tiết kiệm thời gian và chi phí. Tỷ lệ văn bản điện tử trao đổi giữa các cơ quan nhà nước đạt cao, thay thế văn bản giấy tờ truyền thống.
- Đội ngũ cán bộ, công chức khai thác tốt các quy trình xử lý, vận hành, áp dụng chữ ký số trong các hệ thống thông tin, xử lý văn bản điện tử áp dụng chữ ký số.

III.3. Hệ thống giám sát an ninh mạng (GSANM)

- Hệ thống Giám sát an ninh mạng - Ban Cơ yếu Chính phủ có chức năng tổ chức thực hiện giám sát an toàn thông tin trên mạng công nghệ thông tin trọng yếu của các cơ quan Đảng, Nhà nước



III.3. Hệ thống GSANM (tiếp)

- Hệ thống GSANM khi được triển khai tại mạng của các cơ quan Đảng và Nhà nước có chức năng:
  - Phát hiện và ngăn chặn kịp thời các tấn công từ bên ngoài Internet và từ chính bên trong hệ thống mạng
  - Phát hiện và xử lý các điểm yếu, lỗ hổng bảo mật trong hệ thống
  - Phát hiện và xử lý các máy tính trong mạng có các biểu hiện khả nghi (ví dụ: zombie, bùng nổ virus)
  - Thu thập các bằng chứng phục vụ công tác điều tra sau sự cố
  - Theo dõi việc tuân thủ các chính sách an ninh hệ thống
  - Làm tăng hiệu năng hoạt động của mạng
  - Tăng độ sẵn sàng trong việc cung cấp các dịch vụ của mạng
  - Tăng độ an toàn cho dữ liệu trong mạng, giảm thiểu các rủi ro: đánh cắp, sửa đổi, phá hủy dữ liệu
  - Nâng cao nhận thức của người dùng về vấn đề an ninh an toàn cũng như nâng cao chuyên môn nghiệp vụ của đội ngũ làm công tác an ninh mạng, quản trị mạng của mạng khách hàng

III.4. Nghiên cứu, phát triển các ứng dụng công nghệ mới

- Mobile PKI: trong năm 2013 đặc biệt chú trọng đến việc phát triển các giải pháp xác thực bảo mật cho các thiết bị di động

- E-Cloud: Ứng dụng điện toán đám mây vào triển khai PKI và ứng dụng PKI vào xác thực bảo mật điện toán đám mây

- e-Passport: phối hợp với các cơ quan liên quan để phát triển hệ thống PKI cho hộ chiếu điện tử (BCA)

- eDriver License: tiếp tục phối hợp với Bộ GTVT để phát triển GPLX điện tử

- eID: Phối hợp với các cơ quan liên quan để xây dựng hệ thống chứng minh thư điện tử

III.5. Nguồn nhân lực an toàn thông tin

- Nguồn nhân lực luôn là vấn đề cốt lõi trong công tác an toàn, bảo mật thông tin.
- Ngoài nhiệm vụ đào tạo các cán bộ Cơ yếu, Học viện Kỹ thuật Mật mã là Trường đại học đầu tiên đào tạo kỹ sư an toàn thông tin. Được chọn là một trong các trường trọng điểm về an toàn thông tin trong đề án đào tạo chuyên gia an toàn thông tin của Chính phủ. Hàng năm Học viện KTMM đã cung cấp hàng trăm kỹ sư an toàn thông tin được đào tạo bài bản đáp ứng nhu cầu về nguồn nhân lực an toàn thông tin cho cơ quan đảng, nhà nước và xã hội.
- Năm 2012-2013 đã tổ chức đào tạo tại TP.HCM. 2013-2014 đào tạo văn bằng 2 về an toàn thông tin. Hiện đang tổ chức đào tạo riêng cho Thành ủy TP.HCM.
- Hiện đang trình Bộ Giáo dục và Đào tạo mở chương trình đào tạo thạc sỹ an toàn thông tin.

IV. KẾT LUẬN

- Cần tăng cường nâng cao nhận thức của các cán bộ, công chức, viên chức nhà nước về an toàn, bảo mật thông tin. Chủ động nhận biết, ứng phó với những nguy cơ mất an toàn thông tin trong các tình huống cụ thể.
- Ngành Cơ yếu Việt Nam đã và đang triển khai đồng bộ các giải pháp nhằm hiện thực hóa chủ chương, chính sách của Đảng và Nhà nước đảm bảo an toàn và bảo mật thông tin phục vụ sự lãnh đạo, chỉ đạo, điều hành của các ngành, các cấp trong tình hình mới.
- Hạ tầng an ninh, bảo mật trọng yếu (CA, GSANM) đang được Ban Cơ yếu Chính phủ phối hợp với các Bộ, ngành Trung ương và địa phương triển khai mang lại hiệu quả to lớn tạo môi trường làm việc điện tử minh bạch, an toàn, thúc đẩy ứng dụng CNTT, phát triển chính phủ điện tử.
- Phối hợp với Bộ TT&TT giải quyết vấn đề xác thực chéo giữa hệ thống CA chuyên dùng Chính phủ và CA công cộng, liên thông quốc tế…
- Tiếp tục tăng cường sự phối hợp chặt chẽ giữa Ban Cơ yếu Chính phủ và các cơ quan, Bộ, ngành và địa phương triển khai các sản phẩm, giải pháp đảm bảo an toàn thông tin, sử dụng mật mã cơ yếu Việt Nam để bảo vệ thông tin trong các cơ quan Đảng và Nhà nước.

XIN CHÂN THÀNH CẢM ƠN!