

**HỘI THẢO “ĐẨY MẠNH ỨNG DỤNG SẢN PHẨM MẬT MÃ  
DÂN SỰ PHỤC VỤ PHÁT TRIỂN KINH TẾ - XÃ HỘI”**

**MẬT MÃ DÂN SỰ TRONG HỆ THỐNG  
CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG**

---

**Lã Hoàng Trung**  
**Trung tâm Chứng thực điện tử quốc gia**

*Hà Nội, ngày 08 tháng 8 năm 2017*

# Nội dung

1. Tổng quan về dịch vụ chứng thực chữ ký số trong các hoạt động kinh tế - xã hội
2. Thực trạng quản lý các hệ thống cung cấp dịch vụ chứng thực chữ ký số công cộng
3. Ứng dụng sản phẩm và giải pháp bảo mật trong các hệ thống CA công cộng
4. Sự phối hợp giữa Bộ Thông tin và Truyền thông và Ban Cơ yếu Chính phủ trong công tác quản lý nhà nước về dịch vụ chứng thực chữ ký số

# Tổng quan về dịch vụ chứng thực CKS

---

- Khung pháp lý về dịch vụ chứng thực chữ ký số
- Sự phát triển của thị trường dịch vụ chứng thực chữ ký số và việc sử dụng chữ ký số ở Việt Nam
- Một số ứng dụng sử dụng chữ ký số điển hình

# Khung pháp lý về dịch vụ chứng thực CKS

- Luật Giao dịch điện tử ngày 29/11/2005
- Nghị định 26/2007/NĐ-CP ngày 15/02/2007 của Chính phủ quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số
- Nghị định 106/2011/NĐ-CP ngày 23/11/2011 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định 26/2007/NĐ-CP
- Nghị định 170/2013/NĐ-CP ngày 13/11/2013 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định 26/2007/NĐ-CP và Nghị định 106/2011/NĐ-CP
- Các Thông tư hướng dẫn:
  - Thông tư số 37/2009/TT-BTTTT và Thông tư số 08/2011/TT-BTTTT
  - Thông tư số 17/2014/TT-BTTTT
  - Thông tư số 06/2015/TT-BTTTT

# Khung pháp lý về dịch vụ chứng thực CKS

- Các Nghị định chuyên ngành về giao dịch điện tử:
  - Nghị định số 27/2007/NĐ-CP ngày 23/02/2007 của Chính phủ về giao dịch điện tử trong ngành tài chính
  - Nghị định số 87/2012/NĐ-CP ngày 23/10/2012 của Chính phủ quy định chi tiết một số điều của Luật hải quan về thủ tục hải quan điện tử đối với hàng hóa xuất khẩu, nhập khẩu thương mại
  - Nghị định số 52/2013/NĐ-CP ngày 16/5/2013 của Chính phủ về Thương mại điện tử
  - Nghị định số 35/2007/NĐ-CP ngày 08/3/2007 của Chính phủ về giao dịch điện tử trong hoạt động ngân hàng
  - Nghị định số 166/2016/NĐ-CP ngày 24/12/2016 của Chính phủ quy định về giao dịch điện tử trong lĩnh vực bảo hiểm xã hội, bảo hiểm y tế và bảo hiểm thất nghiệp

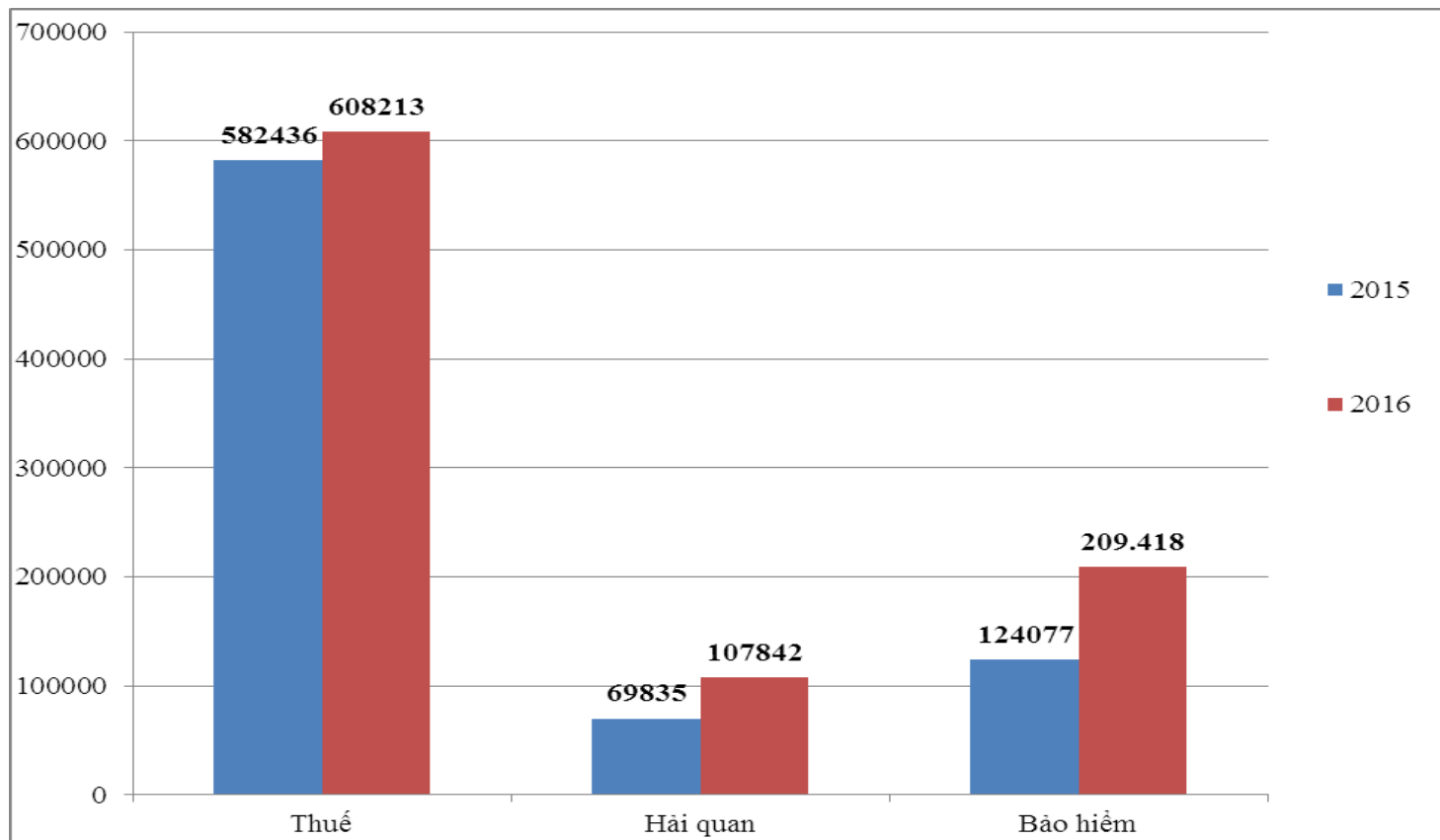
# Sự phát triển của thị trường DVCTCKS

- Các doanh nghiệp cung cấp dịch vụ chứng thực CKS:
  1. VNPT-CA
  2. Viettel-CA
  3. FPT-CA
  4. BKAV-CA
  5. CA2
  6. SmartSign
  7. Newtel-CA
  8. SafeCA
- Số lượng chứng thư số đã cấp:
  - Đến năm 2016, hơn 1,7 triệu chứng thư số công cộng đã được cấp, trong đó, khoảng 840 nghìn CTS đang hoạt động.

# Một số ứng dụng CKS điển hình

- Các ứng dụng sử dụng chữ ký số điển hình (số liệu năm 2016):
  - Hơn 600 nghìn tổ chức, doanh nghiệp sử dụng chữ ký số để kê khai và nộp thuế điện tử
  - Hơn 100 doanh nghiệp sử dụng chữ ký số để khai báo hải quan điện tử
  - Hơn 200 nghìn doanh nghiệp sử dụng chữ ký số để kê khai bảo hiểm xã hội điện tử

# Một số ứng dụng CKS điển hình



So sánh tình hình ứng dụng chữ ký số giai đoạn 2015-2016



# Một số ứng dụng CKS điển hình

- **Kê khai và nộp thuế điện tử**
  - Cơ sở pháp lý:
    - Luật sửa đổi, bổ sung một số điều của Luật Quản lý thuế ngày 20/11/2012
    - Nghị định số 27/2007/NĐ-CP ngày 23/02/2007 của Chính phủ về giao dịch điện tử trong ngành tài chính
    - Thông tư số 110/2015/TT-BTC ngày 28/7/2015 của Bộ Tài chính hướng dẫn giao dịch điện tử trong lĩnh vực thuế
  - Thực tế triển khai

# Một số ứng dụng CKS điển hình

Năm	Số lượng doanh nghiệp kê khai thuế điện tử
2012	105,856
2013	233,601
2014	433,157
2015	582,436
2016	608.213

Năm	Số lượng doanh nghiệp nộp thuế điện tử
2014	17,870
2015	473,022
2016	591.207

# Một số ứng dụng CKS điển hình

- Hải quan điện tử
  - Cơ sở pháp lý:
    - Nghị định 87/2012/NĐ-CP ngày 23/10/2013 của Chính phủ quy định về thủ tục hải quan điện tử đối với hàng hóa xuất nhập khẩu thương mại
  - Thực tế triển khai:
    - 100% các quy trình thủ tục hải quan cơ bản đã được tự động hóa
    - 99,56% doanh nghiệp tham gia thực hiện thủ tục hải quan qua VNACCS/VCIS.

# Một số ứng dụng CKS điển hình

- Hải quan điện tử

Số lượng doanh nghiệp sử dụng dịch vụ công trực tuyến của Tổng cục Hải quan năm 2015 và năm 2016

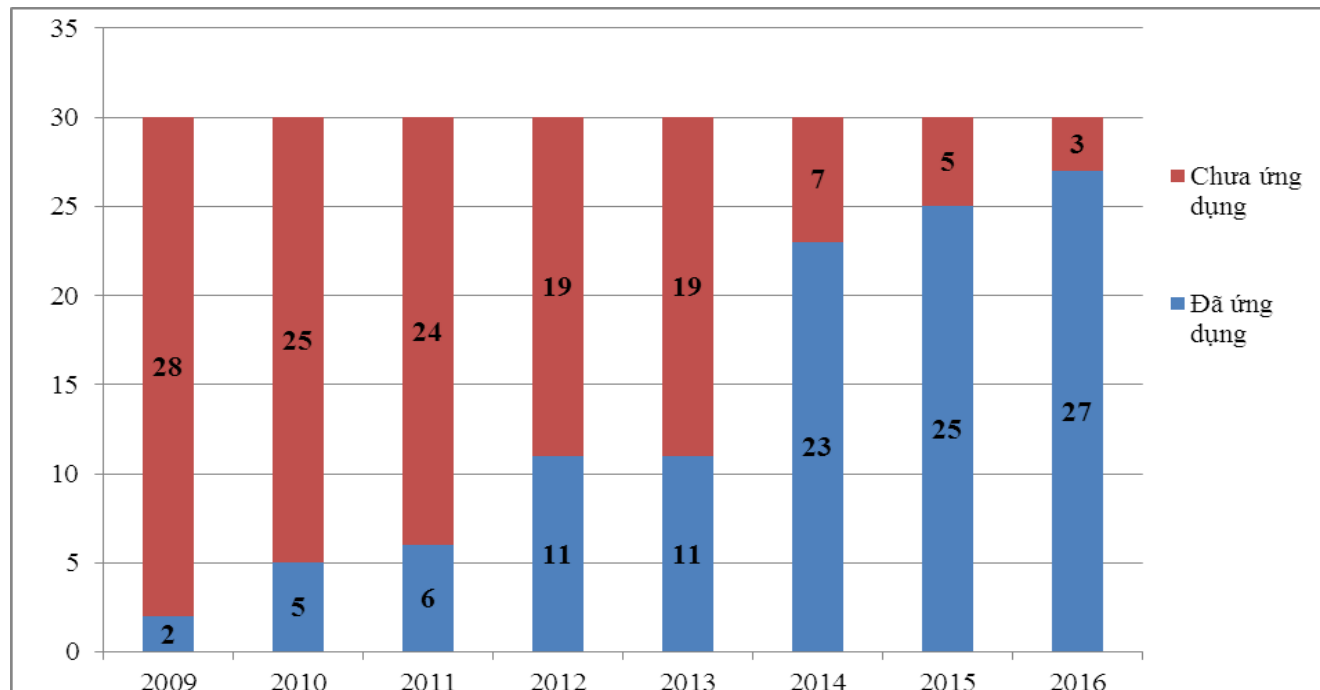
STT	Tên dịch vụ	Năm 2015	Năm 2016
1	Hệ thống thông quan hàng hóa tự động (VNACCS/VCIS)	66.600	97.140
2	Hệ thống Cổng thông tin một cửa quốc gia	3.235	10.702

# Một số ứng dụng CKS điển hình

- **Bảo hiểm xã hội điện tử**
  - Cơ sở pháp lý:
    - Nghị định số 166/2016/NĐ-CP ngày 24/12/2016 của Chính phủ quy định về giao dịch điện tử trong lĩnh vực bảo hiểm xã hội, bảo hiểm y tế và bảo hiểm thất nghiệp
    - Quyết định số 08/2015/QĐ-TTg ngày 09/3/2015 của Thủ tướng Chính phủ về giao dịch điện tử trong thực hiện thủ tục tham gia bảo hiểm.
  - Thực tế triển khai:
    - Năm 2015: 124.077 tổ chức, doanh nghiệp sử dụng chữ ký số để kê khai BHXH điện tử
    - Năm 2015: 209.418 tổ chức, doanh nghiệp sử dụng chữ ký số để kê khai BHXH điện tử

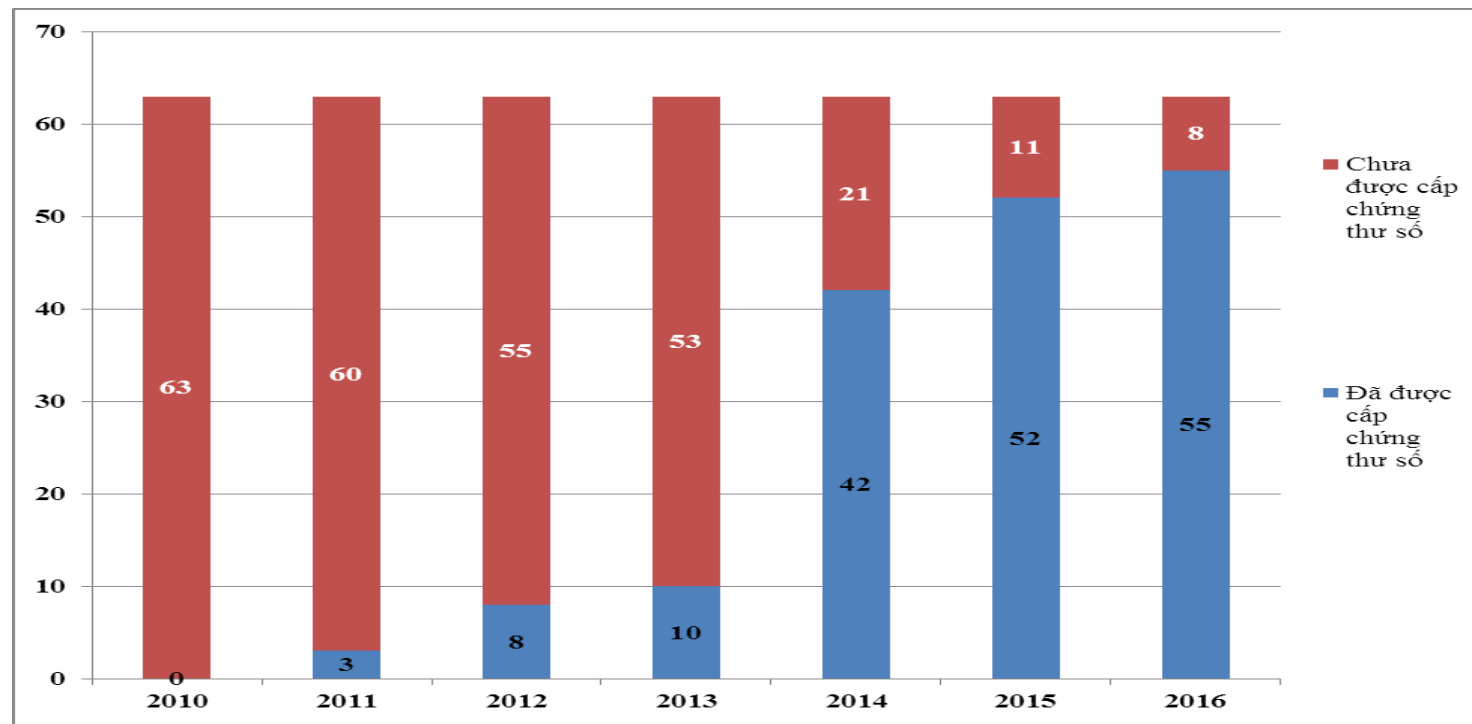
# Sử dụng chữ ký số trong CQNN

- Năm 2016, Ban Cơ yếu Chính phủ đã cấp hơn 64.000 chứng thư số cho các Bộ ngành, cơ quan thuộc Chính phủ và địa phương



Tình hình sử dụng CKS tại các Bộ ngành giai đoạn 2009-2016

# Sử dụng chữ ký số trong CQNN



Tình hình sử dụng CKS tại địa phương giai đoạn 2009-2016

# Quản lý các doanh nghiệp CA

- Nội dung quản lý nhà nước đối với dịch vụ chứng thực chữ ký số:
  1. Xây dựng các văn bản quy phạm pháp luật về chữ ký số và dịch vụ chứng thực chữ ký số;
  2. Xây dựng chính sách, chiến lược, quy hoạch, kế hoạch phát triển và quản lý dịch vụ chứng thực chữ ký số tại Việt Nam;
  3. Chủ trì, phối hợp với Bộ Công an, Ban Cơ yếu Chính phủ trong việc quản lý các tổ chức cung cấp dịch vụ chứng thực chữ ký số; thanh tra, kiểm tra và xử lý vi phạm;
  4. Chủ trì, phối hợp với Bộ Khoa học và Công nghệ, Bộ Công an, Ban Cơ yếu Chính phủ xây dựng và ban hành các quy chuẩn kỹ thuật và tiêu chuẩn bắt buộc áp dụng về chữ ký số, dịch vụ chứng thực chữ ký số và ứng dụng chữ ký số;



# Quản lý các doanh nghiệp CA

- Nội dung quản lý nhà nước đối với dịch vụ chứng thực chữ ký số (tiếp):
  5. Quản lý, vận hành và duy trì hoạt động của tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia;
  6. Thực hiện quản lý thuê bao, chứng thư số nước ngoài được chấp nhận tại Việt Nam, kiểm tra việc sử dụng chứng thư số nước ngoài được chấp nhận tại Việt Nam;
  7. Ban hành các quy định, hướng dẫn, tiêu chuẩn kỹ thuật liên quan đến việc liên thông giữa các tổ chức cung cấp dịch vụ chứng thực chữ ký số.

# Quản lý các doanh nghiệp CA

- Thực tế triển khai công tác quản lý nhà nước đối với các doanh nghiệp CA:
  - Cấp phép
  - Thu hồi giấy phép
  - Cấp chứng thư số
  - Ban hành tiêu chuẩn kỹ thuật
  - Xử lý vi phạm: thanh tra, kiểm tra
  - Xây dựng và ban hành văn bản quy phạm pháp luật, chính sách về chữ ký số, dịch vụ chứng thực chữ ký số

# Ứng dụng sản phẩm và giải pháp bảo mật trong các hệ thống CA công cộng

- Danh sách các thiết bị phần cứng phục vụ an toàn, bảo mật của các hệ thống CA công cộng (1)
  - HSM (khối an ninh phần cứng HSM): là thiết bị phục vụ việc tạo và lưu trữ cặp khóa của các CA.
  - Một số nhà cung cấp HSM thông dụng:
    - Thales nShield của hãng Thales
    - Utimaco CryptoServer của hãng Utimaco
    - AEP Keyper của hãng AEP
    - Safenet Luna của hãng SafeNet/Gemalto
- USB Token: thiết bị phục vụ việc tạo và lưu trữ cặp khóa của thuê bao

# Ứng dụng sản phẩm và giải pháp bảo mật trong các hệ thống CA công cộng

- Danh sách các thiết bị phần cứng phục vụ an toàn, bảo mật của các hệ thống CA công cộng (2)
  - Firewall
    - Một số nhà cung cấp giải pháp Firewall thông dụng:
      - Firewall Juniper: SRX110H2-VA, SRX220H2, SRX300, SRX340
      - Firewall Fortinet: 60D, 100D, ...
      - Firewall Cisco: 5506, 5508,
  - Firewall mới có thêm tính năng phát hiện, phòng chống tấn công (IPS) như Firewall Cisco

# Ứng dụng sản phẩm và giải pháp bảo mật trong các hệ thống CA công cộng

- Danh sách các phần mềm phục vụ an toàn, bảo mật của các hệ thống CA công cộng
  - Hệ thống phát hiện và tự động ngăn chặn tấn công từ bên ngoài Internet vào hệ thống mạng
    - Thường tích hợp IDS/IPS vào Firewall
    - Phần mềm IDS phổ biến hiện nay là Snort
    - Cisco IOS IPS
  - Các phần mềm Anti-virus

# Việc đáp ứng quy định tại Thông tư 06/2015/TT-BTTTT

- Các thiết bị phần cứng
  - HSM
    - Yêu cầu của Thông tư 06: FIPS PUB 140-2 level 3
    - Thông số thực tế
      - AEP Keyper: FIPS PUB 140-2 level 4
      - Thales nShield: FIPS PUB 140-2 level 3
      - Utimaco CryptoServer: FIPS PUB 140-2 level 3
      - ...
  - USB Token
    - Yêu cầu của Thông tư 06: FIPS PUB 140-2 level 2
    - Thông số thực tế: đáp ứng FIPS PUB 140-2 level 2

# Phối hợp giữa Bộ TTTT và Ban Cơ yếu CP

- Phối hợp trong thời gian vừa qua:
  - Thẩm tra hồ sơ cấp giấy phép cung cấp dịch vụ chứng thực chữ ký số công cộng cho 08 doanh nghiệp.
  - Kiểm tra, đánh giá tình hình ứng dụng chữ ký số trong cơ quan nhà nước các năm 2014, 2016, 2017

# Phối hợp giữa Bộ TTTT và Ban Cơ yếu CP

- Đề xuất phối hợp trong thời gian tới:
  - Kiểm tra các doanh nghiệp CA về việc đáp ứng danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo Thông tư số 06/2015/TT-BTTTT, đặc biệt là kiểm tra các thiết bị phần cứng.
  - Nghiên cứu khoa học: các đề tài nghiên cứu về mật mã dân sự, về ứng dụng mật mã dân sự trong các hệ thống chứng thực chữ ký số...



---

**TRÂN TRỌNG CẢM ƠN**