

BỘ THÔNG TIN VÀ TRUYỀN THÔNG**BỘ THÔNG TIN
VÀ TRUYỀN THÔNG****CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc**

Số: 41/2017/TT-BTTTT

Hà Nội, ngày 19 tháng 12 năm 2017

THÔNG TƯ**Quy định sử dụng chữ ký số
cho văn bản điện tử trong cơ quan nhà nước**

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Nghị định số 26/2007/NĐ-CP ngày 15 tháng 02 năm 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 số 106/2011/NĐ-CP ngày 23 tháng 11 năm 2011 sửa đổi, bổ sung một số điều của Nghị định số 26/2007/NĐ-CP của Chính phủ ngày 15 tháng 02 năm 2007; Nghị định số 170/2013/NĐ-CP ngày 13 tháng 11 năm 2013 sửa đổi, bổ sung một số điều của Nghị định số 26/2007/NĐ-CP ngày 15 tháng 02 năm 2007 và Nghị định số 106/2011/NĐ-CP ngày 23 tháng 11 năm 2011 của Chính phủ;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 01/2013/NĐ-CP ngày 03 tháng 01 năm 2013 của Chính phủ quy định chi tiết thi hành một số điều của Luật Lưu trữ;

Căn cứ Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Bộ trưởng Bộ Thông tin và Truyền thông ban hành Thông tư quy định sử dụng chữ ký số cho văn bản điện tử trong cơ quan nhà nước.

Chương I**QUY ĐỊNH CHUNG****Điều 1. Phạm vi điều chỉnh**

1. Thông tư này quy định về ký số, kiểm tra chữ ký số trên văn bản điện tử; yêu cầu kỹ thuật và chức năng của phần mềm ký số, phần mềm kiểm tra chữ ký số cho văn bản điện tử trong cơ quan nhà nước.

2. Thông tư này không quy định việc sử dụng chữ ký số cho văn bản điện tử chứa thông tin thuộc danh mục bí mật nhà nước.

Điều 2. Đối tượng áp dụng

1. Thông tư này được áp dụng đối với các cơ quan, tổ chức (bao gồm: các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các cấp, các đơn vị sự nghiệp sử dụng ngân sách nhà nước) và tổ chức, cá nhân liên quan sử dụng chữ ký số cho văn bản điện tử của cơ quan nhà nước.

2. Khuyến khích các cơ quan, tổ chức khác áp dụng.

Điều 3. Giải thích từ ngữ

Trong Thông tư này, các từ ngữ dưới đây được hiểu như sau:

1. "Chứng thư số cơ quan, tổ chức" là chứng thư số do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp cho người đứng đầu cơ quan, tổ chức theo quy định của pháp luật.

2. "Chứng thư số cá nhân" là chứng thư số do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp cho các chức danh nhà nước, người có thẩm quyền của cơ quan, tổ chức theo quy định của pháp luật về quản lý và sử dụng con dấu.

3. "Khóa bí mật con dấu" là khóa bí mật tương ứng với chứng thư số cơ quan, tổ chức.

4. "Khóa bí mật cá nhân" là khóa bí mật tương ứng với chứng thư số cá nhân.

5. "Chữ ký số cơ quan, tổ chức" là chữ ký số được tạo ra khi sử dụng khóa bí mật con dấu.

6. "Chữ ký số cá nhân" là chữ ký số được tạo ra khi sử dụng khóa bí mật cá nhân.

7. "Phần mềm ký số" là chương trình phần mềm có chức năng ký số vào văn bản điện tử.

8. "Phần mềm kiểm tra chữ ký số" là chương trình phần mềm có chức năng kiểm tra tính hợp lệ của chữ ký số trên văn bản điện tử.

9. "Tính xác thực của văn bản điện tử ký số" là văn bản điện tử thông qua chữ ký số được ký số gắn với văn bản điện tử xác định được người ký số hoặc cơ quan, tổ chức ký số vào văn bản điện tử.

10. "Tính toàn vẹn của văn bản điện tử ký số" là văn bản điện tử sau khi được ký số nội dung không bị thay đổi trong suốt quá trình trao đổi, xử lý và lưu trữ.

11. "Hệ thống kiểm tra trạng thái chứng thư số trực tuyến" (OCSP) là hệ thống cung cấp dịch vụ cho phép xác định trạng thái hiện thời của chứng thư số.

12. "Thiết bị lưu khóa bí mật" là thiết bị vật lý chứa khóa bí mật và chứng thư số của thuê bao.

Điều 4. Nguyên tắc sử dụng chữ ký số cho văn bản điện tử

1. Chữ ký số phải gắn kèm văn bản điện tử sau khi ký số.
2. Văn bản điện tử được ký số phải đảm bảo tính xác thực, tính toàn vẹn xuyên suốt quá trình trao đổi, xử lý và lưu trữ văn bản điện tử được ký số.

Điều 5. Quản lý khóa bí mật cá nhân và khóa bí mật con dấu

1. Người có thẩm quyền ký số có trách nhiệm bảo quản an toàn khóa bí mật cá nhân.
2. Người đứng đầu cơ quan, tổ chức có trách nhiệm giao cho nhân viên văn thư quản lý, sử dụng khóa bí mật con dấu theo quy định.
3. Thiết bị lưu khóa bí mật con dấu phải được cất giữ an toàn tại trụ sở cơ quan, tổ chức.

Chương II

QUY ĐỊNH VỀ KÝ SỐ, KIỂM TRA CHỮ KÝ SỐ TRÊN VĂN BẢN ĐIỆN TỬ TRONG CƠ QUAN NHÀ NƯỚC

Điều 6. Ký số trên văn bản điện tử

1. Việc ký số được thực hiện thông qua phần mềm ký số; việc ký số vào văn bản điện tử thành công hoặc không thành công phải được thông báo thông qua phần mềm.

2. Ký số trên văn bản điện tử

a) Trường hợp quy định người có thẩm quyền ký số trên văn bản điện tử, thông qua phần mềm ký số, người có thẩm quyền sử dụng khóa bí mật cá nhân để thực hiện việc ký số vào văn bản điện tử;

b) Trường hợp quy định cơ quan, tổ chức ký số trên văn bản điện tử, thông qua phần mềm ký số, văn thư được giao sử dụng khóa bí mật con dấu của cơ quan, tổ chức để thực hiện việc ký số vào văn bản điện tử.

3. Hiện thị thông tin về chữ ký số của người có thẩm quyền và chữ ký số của cơ quan, tổ chức trên văn bản điện tử thực hiện theo quy định của Bộ Nội vụ.

4. Thông tin về người có thẩm quyền ký số, cơ quan, tổ chức ký số phải được quản lý trong cơ sở dữ liệu đi kèm phần mềm ký số. Nội dung thông tin quản lý quy định tại khoản 4, Điều 1, Nghị định số 106/2011/NĐ-CP ngày 23 tháng 11 năm 2011 của Chính phủ.

Điều 7. Kiểm tra chữ ký số trên văn bản điện tử

1. Kiểm tra chữ ký số trên văn bản điện tử thực hiện như sau:

- a) Giải mã chữ ký số bằng khóa công khai tương ứng;
- b) Kiểm tra, xác thực thông tin của người ký số trên chứng thư số gắn kèm văn bản điện tử; việc kiểm tra, xác thực thông tin người ký số được thực hiện theo Điều 8 Thông tư này;
- c) Kiểm tra tính toàn vẹn của văn bản điện tử ký số.

2. Chữ ký số trên văn bản điện tử là hợp lệ khi việc kiểm tra, xác thực thông tin về chứng thư số của người ký số tại thời điểm ký còn hiệu lực, chữ ký số được tạo ra đúng bởi khóa bí mật tương ứng với khóa công khai trên chứng thư số và văn bản điện tử đảm bảo tính toàn vẹn.

3. Thông tin về người ký số; cơ quan, tổ chức ký số trên văn bản điện tử phải được quản lý trong cơ sở dữ liệu đi kèm phần mềm kiểm tra chữ ký số. Nội dung thông tin quản lý quy định tại khoản 4, Điều 1, Nghị định số 106/2011/NĐ-CP ngày 23 tháng 11 năm 2011 của Chính phủ.

Điều 8. Kiểm tra hiệu lực của chứng thư số

1. Thực hiện kiểm tra hiệu lực của chứng thư số tại thời điểm ký số thực hiện theo các bước sau:

a) Kiểm tra hiệu lực chứng thư số qua danh sách chứng thư số bị thu hồi (CRL) được công bố tại thời điểm ký số hoặc kiểm tra hiệu lực chứng thư số bằng phương pháp kiểm tra trạng thái chứng thư số trực tuyến (OCSP) ở chế độ trực tuyến;

b) Việc kiểm tra chứng thư số của người ký số trên văn bản điện tử phải kiểm tra đến tận tổ chức cung cấp dịch vụ chứng thực chữ ký số gốc (Root CA).

2. Chứng thư số có hiệu lực khi đáp ứng tất cả các tiêu chí sau:

- a) Có hiệu lực tại thời điểm ký;

b) Phù hợp phạm vi sử dụng của chứng thư số và trách nhiệm pháp lý của người ký;

c) Trạng thái của chứng thư số còn hoạt động tại thời điểm ký số.

3. Chứng thư số không có hiệu lực khi không đáp ứng một trong các tiêu chí tại khoản 2 Điều này.

Điều 9. Thông tin lưu trữ kèm theo văn bản điện tử ký số

1. Thông tin lưu trữ kèm theo văn bản điện tử ký số, bao gồm:

a) Đối với văn bản gửi đi:

- Chứng thư số của người ký số tại thời điểm ký;
- Danh sách chứng thư số thu hồi tại thời điểm ký của tổ chức cung cấp dịch vụ chứng thực chữ ký số;

- Quy chế chứng thực của tổ chức cung cấp dịch vụ chứng thực chữ ký số vào thời điểm ký;

- Thông tin về trách nhiệm của người ký;

- Chứng thực dấu thời gian hợp lệ vào thời điểm ký.

b) Đối với văn bản đến:

- Các chứng thư số tương ứng với các chữ ký số trên văn bản điện tử đến;

- Danh sách thu hồi chứng thư số vào thời điểm ký của tổ chức cung cấp dịch vụ chứng thực chữ ký số;

- Quy chế chứng thực của tổ chức cung cấp dịch vụ chứng thực chữ ký số vào thời điểm ký;

- Thông tin về trách nhiệm của người ký;

- Chứng thực dấu thời gian hợp lệ vào thời điểm nhận.

3. Thông tin lưu trữ kèm theo văn bản điện tử được quản lý bằng phần mềm ký số, phần mềm kiểm tra chữ ký số phù hợp thời gian lưu trữ của văn bản điện tử theo quy định.

Điều 10. Hủy bỏ thông tin lưu trữ kèm theo văn bản điện tử ký số

1. Thông tin lưu trữ kèm theo văn bản điện tử bị hủy bỏ đồng thời với văn bản điện tử.

2. Việc hủy bỏ thông tin lưu trữ kèm theo văn bản điện tử ký số không được làm ảnh hưởng đến các văn bản điện tử khác và đảm bảo sự hoạt động bình thường của hệ thống.

3. Hủy bỏ thông tin lưu trữ kèm theo văn bản điện tử ký số được thực hiện bằng phần mềm.

Chương III

YÊU CẦU KỸ THUẬT VÀ CHỨC NĂNG

ĐỐI VỚI PHẦN MỀM KÝ SỐ, KIỂM TRA CHỮ KÝ SỐ

Điều 11. Yêu cầu kỹ thuật và chức năng đối với phần mềm ký số

Phần mềm ký số là phần mềm độc lập hoặc một thành phần (module) phần mềm đáp ứng các yêu cầu sau:

1. Đáp ứng các tiêu chuẩn, quy chuẩn kỹ thuật quy định tại phụ lục kèm theo Thông tư này.

2. Có các chức năng ký số trên văn bản điện tử đáp ứng quy định tại khoản 2, 3 và 4 Điều 6 Thông tư này.

3. Có chức năng kiểm tra hiệu lực chứng thư số quy định tại Điều 8 Thông tư này.

4. Có chức năng quản lý thông tin lưu trữ kèm theo văn bản điện tử ký số quy định tại Điều 9 Thông tư này.

5. Có chức năng hủy bỏ thông tin lưu trữ kèm theo văn bản điện tử ký số quy định tại Điều 10 Thông tư này.

6. Có chức năng thông báo (bằng chữ/bằng ký hiệu) cho người ký số biết việc ký số vào văn bản điện tử thành công hay không thành công.

7. Hỗ trợ cài đặt, tích hợp chứng thư số gốc của tổ chức chứng thực chữ ký số cấp chứng thư số để ký số văn bản điện tử vào phần mềm ký số để kiểm tra hiệu lực chứng thư số trên văn bản điện tử.

8. Đóng dấu thời gian tại thời điểm ký số.

Điều 12. Yêu cầu kỹ thuật và chức năng đối với phần mềm kiểm tra chữ ký số

Phần mềm kiểm tra chữ ký số là phần mềm độc lập hoặc một thành phần (module) phần mềm có các chức năng kiểm tra chữ ký số trên văn bản điện tử đáp ứng các yêu cầu sau:

1. Đáp ứng các tiêu chuẩn, quy chuẩn kỹ thuật quy định tại phụ lục kèm theo Thông tư này.
2. Có chức năng kiểm tra chữ ký số trên văn bản điện tử quy định tại khoản 1, 2 và 3 Điều 7 Thông tư này.
3. Có chức năng quản lý thông tin lưu trữ kèm theo văn bản điện tử ký số quy định tại Điều 9 Thông tư này.
4. Có chức năng hủy bỏ thông tin kèm theo văn bản điện tử ký số quy định tại Điều 10 Thông tư này.
5. Hỗ trợ cài đặt, tích hợp chứng thư số gốc của tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp chứng thư số để ký số văn bản điện tử vào phần mềm kiểm tra chữ ký số để kiểm tra chữ ký số trên văn bản điện tử.
6. Có chức năng thông báo kết quả kiểm tra chữ ký số là hợp lệ hoặc không hợp lệ cho người kiểm tra biết.
7. Đóng dấu thời gian tại thời điểm tiếp nhận văn bản đến.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 13. Trách nhiệm của tổ chức cung cấp dịch vụ chứng thực chữ ký số

1. Lưu trữ đầy đủ, chính xác, cập nhật, công bố toàn bộ các thông tin sau đây trên trang tin điện tử (website) của tổ chức cung cấp dịch vụ chứng thực chữ ký số và trang tin điện tử phải đảm bảo hoạt động 24 giờ trong ngày và 7 ngày trong tuần (để hỗ trợ xác định tính hợp lệ của chữ ký số trên văn bản điện tử)
 - a) Thông tin liên quan đến hoạt động tạm dừng, thu hồi chứng thư số và các chứng thư số bị thu hồi của thuê bao;
 - b) Thông tin liên quan đến chứng thư số của thuê bao, danh sách các chứng thư số có hiệu lực hoặc đã hết hiệu lực;
 - c) Quy chế chứng thực của tổ chức cung cấp dịch vụ chứng thực chữ ký số.
2. Công bố các đặc tả kỹ thuật (cả tài liệu và bộ công cụ) liên quan đến tổ chức cung cấp dịch vụ chứng thực chữ ký số và các tiêu chuẩn chữ ký số; cung cấp chứng thư số gốc của tổ chức cung cấp dịch vụ chứng thực chữ ký số cho các nhà phát triển phần mềm để tích hợp vào phần mềm kiểm tra chữ ký số.

3. Khuyến khích tổ chức cung cấp dịch vụ chứng thực chữ ký số cung cấp dịch vụ kiểm tra trạng thái chứng thư số trực tuyến (OCSP).

4. Cung cấp dịch vụ cấp dấu thời gian.

Điều 14. Trách nhiệm của cơ quan, tổ chức sử dụng chữ ký số cho văn bản điện tử

1. Ứng dụng phần mềm ký số, phần mềm kiểm tra chữ ký số quy định tại các Điều 11 và 12 Thông tư này.

2. Triển khai kết nối mạng theo quy định tại khoản 3, Điều 8, Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ đảm bảo an toàn, bảo mật và tính sẵn sàng cao.

3. Tổ chức quản lý các sản phẩm phần mềm (theo phiên bản) có chức năng ký số, kiểm tra chữ ký số, lưu trữ thông tin kèm theo văn bản điện tử ký số tương ứng với tiêu chuẩn, quy chuẩn kỹ thuật về chữ ký số mà phần mềm hỗ trợ nhằm đảm bảo tính sẵn sàng, tương thích và an toàn bảo mật trong quá trình sử dụng văn bản điện tử ký số đã lưu trữ.

Điều 15. Trách nhiệm của người đứng đầu cơ quan, tổ chức sử dụng chữ ký số

1. Thực hiện trách nhiệm của người đứng đầu quy định tại khoản 1, Điều 8, Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ.

2. Thường xuyên kiểm tra nhằm đảm bảo việc quản lý, sử dụng chữ ký số, chứng thư số tại cơ quan, tổ chức mình được thực hiện theo Thông tư này và các quy định khác có liên quan.

3. Căn cứ vào yêu cầu tổ chức, nghiệp vụ và đảm bảo an toàn thông tin trong giao dịch điện tử đề xuất cấp, thu hồi, tạm dừng chứng thư số cá nhân và chứng thư số cơ quan, tổ chức thuộc quyền quản lý.

4. Khi có yêu cầu chuyển đổi văn bản điện tử ký số đang được lưu trữ sang định dạng tệp văn bản mới (vì nguyên nhân an toàn thông tin hoặc vì sự lỗi thời của phần cứng, phần mềm), phải xây dựng phương án và được phê duyệt bởi cơ quan chuyên trách về công nghệ thông tin, đảm bảo khả năng tương thích và xác thực hiệu lực của chữ ký số.

Điều 16. Điều khoản chuyển tiếp

Chậm nhất sau 12 tháng kể từ ngày Thông tư có hiệu lực thi hành, các cơ quan, tổ chức đang sử dụng các phần mềm có chức năng ký số, kiểm tra chữ ký số chưa đáp ứng yêu cầu kỹ thuật và chức năng quy định tại Thông tư này thực hiện việc nâng cấp, bổ sung phần mềm ký số, phần mềm kiểm tra chữ ký số để đáp ứng quy định.

Điều 17. Điều khoản thi hành

1. Trung tâm Chứng thực điện tử quốc gia có trách nhiệm chủ trì, phối hợp với Vụ Pháp chế và các đơn vị có liên quan hướng dẫn, hỗ trợ kỹ thuật việc thực hiện các nội dung của Thông tư này.

2. Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương, các đơn vị chuyên trách về công nghệ thông tin các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ có trách nhiệm:

a) Phổ biến việc thực hiện các quy định của Thông tư này;

b) Hàng năm báo cáo Bộ Thông tin và Truyền thông (Trung tâm Chứng thực điện tử quốc gia) về tình hình sử dụng chữ ký số cho văn bản điện tử tại cơ quan, tổ chức.

Điều 18. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày 05 tháng 02 năm 2018.

2. Chánh Văn phòng, Giám đốc Trung tâm Chứng thực điện tử quốc gia, cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này.

4. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, các cơ quan, tổ chức và cá nhân phản ánh kịp thời về Bộ Thông tin và Truyền thông (Trung tâm Chứng thực điện tử quốc gia) để xem xét, giải quyết./.

BỘ TRƯỞNG

Trương Minh Tuấn

BỘ THÔNG TIN VÀ TRUYỀN THÔNG CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHỤ LỤC
DANH MỤC TIÊU CHUẨN
VỀ CHỮ KÝ SỐ VÀ ĐỊNH DẠNG VĂN BẢN ĐIỆN TỬ KÝ SỐ
(Ban hành kèm theo Thông tư số 41/2017/TT-BTTTT ngày 19 tháng 12 năm 2017
của Bộ trưởng Bộ Thông tin và Truyền thông)

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1	Tiêu chuẩn về định dạng văn bản điện tử			
1.1	Văn bản điện tử ký số (đáp ứng yêu cầu tại Điều 6 Thông tư này)	(.pdf)	Định dạng Portable Document (.pdf) - Version 1.4 trở lên	Bắt buộc áp dụng
1.2	Định dạng văn bản điện tử ký số khác bao gồm: văn bản, bảng tính, trình diễn, ảnh đồ họa	Tiêu chuẩn về văn bản, bảng tính, trình diễn, ảnh đồ họa thuộc danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước		Khuyến khích áp dụng
2	Tiêu chuẩn về chữ ký số			
2.1	Tiêu chuẩn mật mã chữ ký số	PKCS#1	RSA Cryptography Standard (Phiên bản 2.1 trở lên)	Bắt buộc áp dụng
		TCVN 7635:2007	Các kỹ thuật mật mã - Chữ ký số	
2.2	Tiêu chuẩn hàm băm an toàn	FIPS PUB 180-4	Secure Hash Standard	Bắt buộc áp dụng hàm băm SHA-256, 384, 512.
2.3	An toàn trao đổi bản tin XML	XML Encryption Syntax and Processing	XML Encryption Syntax and Processing	Bắt buộc áp dụng

		XML Signature Syntax and Processing	XML Signature Syntax and Processing	Bắt buộc áp dụng
2.4	Quản lý khóa công khai bản tin XML	XKMS v2.0	XML Key Management Specification version 2.0	Bắt buộc áp dụng
2.5	Chuẩn cú pháp thông điệp mật mã cho ký số và mã hóa	PKCS#7 v1.5 (RFC 2315)	Cryptographic message syntax for file-based signing and encrypting	Bắt buộc áp dụng
3	Tiêu chuẩn dịch vụ cấp dấu thời gian			
3.1	Giao thức cấp dấu thời gian	RFC 3161	Internet X.509 Public Key Infrastructure - Time stamp Protocol	Bắt buộc áp dụng
3.2	Dịch vụ cấp dấu thời gian	ISO/IEC 18014-1:2008	Information technology - Security techniques - Time Stamping services - Part 1: Framework	Bắt buộc áp dụng - Áp dụng bộ ba tiêu chuẩn: ISO/IEC 18014-1:2008); ISO/IEC 18014-2:2009); ISO/IEC 18014-3:2009.
		ISO/IEC 18014-2:2009	Information technology - Security techniques - Time Stamping services - Part 2: Mechanisms producing independent tokens	
		ISO/IEC 18014-3:2009	Information technology - Security techniques - Time-stamping services - Part 3: Mechanisms producing linked tokens	