

Số: *22* /2020/TT-BTTTT

Hà Nội, ngày *07* tháng *9* năm 2020

THÔNG TƯ

**Quy định về yêu cầu kỹ thuật đối với phần mềm ký số,
phần mềm kiểm tra chữ ký số**

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

Căn cứ Nghị định số 130/2018/NĐ-CP ngày 27 tháng 9 năm 2018 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;

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;

Theo đề nghị của Giám đốc Trung tâm Chứng thực điện tử quốc gia,

Bộ trưởng Bộ Thông tin và Truyền thông ban hành Thông tư quy định về yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số.

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

1. Thông tư này quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số.

2. Yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số cho văn bản điện tử trong cơ quan nhà nước không thuộc phạm vi điều chỉnh của Thông tư này.

Điều 2. Đối tượng áp dụng

1. Thông tư này áp dụng đối với cơ quan, tổ chức, cá nhân lựa chọn sử dụng phần mềm ký số, phần mềm kiểm tra chữ ký số trong giao dịch điện tử; các tổ chức cung cấp dịch vụ chứng thực chữ ký số; các tổ chức, cá nhân phát triển ứng dụng, sử dụng chữ ký số.

2. Thông tư này không áp dụng đối với tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ.

Điều 3. Giải thích từ ngữ

1. "Chứng thư số tổ chức" là một dạng chứng thư điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp nhằm cung cấp thông tin định danh cho khóa công khai của một cơ quan, tổ chức từ đó xác nhận cơ quan, tổ chức là người ký chữ ký số bằng việc sử dụng khóa bí mật tương ứng.

2. "Chứng thư số cá nhân" là một dạng chứng thư điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp nhằm cung cấp thông tin định danh cho khóa công khai của một cá nhân, từ đó xác nhận cá nhân là người ký chữ ký số bằng việc sử dụng khóa bí mật tương ứng.

3. "Khóa bí mật tổ chức" là khóa bí mật tương ứng với chứng thư số tổ chức.

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

5. "Phần mềm ký số" là chương trình phần mềm độc lập hoặc một thành phần (module) phần mềm hoặc giải pháp có chức năng ký số vào thông điệp dữ liệu.

6. "Phần mềm kiểm tra chữ ký số" là chương trình phần mềm độc lập hoặc một thành phần (module) phần mềm hoặc giải pháp có chức năng kiểm tra tính hợp lệ của chữ ký số trên thông điệp dữ liệu ký số.

7. "Đường dẫn tin tưởng của chứng thư số" là thông tin đường dẫn địa chỉ internet trên chứng thư số cho biết tổ chức cung cấp dịch vụ chứng thực chữ ký số đã cấp phát ra chứng thư số đó.

Chương II

YÊU CẦU KỸ THUẬT ĐỐI VỚI PHẦN MỀM KÝ SỐ, PHẦN MỀM KIỂM TRA CHỮ KÝ SỐ

Mục 1- Phần mềm ký số

Điều 4. Yêu cầu chung

Tuân thủ các tiêu chuẩn kỹ thuật về chữ ký số trên thông điệp dữ liệu tại Phụ lục Danh mục tiêu chuẩn kỹ thuật về chữ ký số trên thông điệp dữ liệu kèm theo Thông tư này.

Điều 5. Yêu cầu chức năng

1. Chức năng ký số:

a) Trường hợp người ký số trên thông điệp dữ liệu là cá nhân, cho phép người ký số sử dụng khóa bí mật cá nhân để thực hiện việc ký số vào thông điệp dữ liệu;

b) Trường hợp người ký số trên thông điệp dữ liệu là tổ chức, cho phép người ký số sử dụng khóa bí mật tổ chức để thực hiện việc ký số vào thông điệp dữ liệu.

2. Chức năng kiểm tra hiệu lực của chứng thư số:

a) Cho phép việc kiểm tra chứng thư số của người ký số trên thông điệp dữ liệu phải kiểm tra theo đường dẫn tin tưởng trên chứng thư số và phải thực hiện đến tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia.

b) Nội dung kiểm tra hiệu lực của chứng thư số tại thời điểm ký số:

- Thời gian có hiệu lực của chứng thư số;

- Trạng thái chứng thư số qua danh sách chứng thư số thu hồi (CRL) được công bố tại thời điểm ký số hoặc bằng phương pháp kiểm tra trạng thái chứng thư số trực tuyến (OCSP) ở chế độ trực tuyến trong trường hợp tổ chức cung cấp dịch vụ chứng thực chữ ký số có cung cấp dịch vụ OCSP;

- Thuật toán mật mã trên chứng thư số;

- Mục đích, phạm vi sử dụng của chứng thư số.

c) Hiệu lực của chứng thư số khi đáp ứng tất cả các tiêu chí sau:

- Thời gian trên chứng thư số còn hiệu lực tại thời điểm ký số;

- Các thuật toán mật mã trên chứng thư số tuân thủ theo quy định về quy chuẩn, tiêu chuẩn kỹ thuật bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số đang có hiệu lực;

- Trạng thái của chứng thư số còn hoạt động tại thời điểm ký số;

- Chứng thư số được sử dụng đúng mục đích, phạm vi sử dụng.

3. Chức năng lưu trữ và hủy bỏ các thông tin sau kèm theo thông điệp dữ liệu ký số:

a) Chứng thư số tương ứng với khóa bí mật mà người ký số sử dụng để ký thông điệp dữ liệu tại thời điểm ký số;

b) Danh sách chứng thư số thu hồi tại thời điểm ký của tổ chức cung cấp dịch vụ chứng thực chữ ký số đã cấp chứng thư số để ký số tương ứng với chữ ký số trên thông điệp dữ liệu đi;

c) Quy chế chứng thực của tổ chức cung cấp dịch vụ chứng thực chữ ký số đã cấp chứng thư số tương ứng với chữ ký số trên thông điệp dữ liệu đi;

d) Kết quả kiểm tra trạng thái chứng thư số tương ứng với chữ ký số trên thông điệp dữ liệu được gửi đến.

4. Chức năng thay đổi (thêm, bớt) chứng thư số của tổ chức cung cấp dịch vụ chứng thực chữ ký số.

5. Chức năng thông báo (bằng chữ/bằng ký hiệu) cho người ký số biết việc ký số vào thông điệp dữ liệu thành công hay không thành công.

Mục 2-Phần mềm kiểm tra chữ ký số

Điều 6. Yêu cầu chung

Tuân thủ các tiêu chuẩn kỹ thuật về chữ ký số trên thông điệp dữ liệu tại Phụ lục Danh mục tiêu chuẩn về chữ ký số trên thông điệp dữ liệu kèm theo Thông tư này.

Điều 7. Yêu cầu chức năng

1. Chức năng kiểm tra tính hợp lệ của chữ ký số trên thông điệp dữ liệu:

a) Cho phép xác minh chữ ký số trên thông điệp dữ liệu theo nguyên tắc chữ ký số được tạo ra đúng với khóa bí mật tương ứng với khóa công khai trên chứng thư số;

b) Cho phép việc kiểm tra chứng thư số của người ký số trên thông điệp dữ liệu phải kiểm tra theo đường dẫn tin tưởng trên chứng thư số và phải thực hiện đến tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia.

c) Cho phép kiểm tra, xác thực thông tin của người ký số trên thông điệp dữ liệu thực hiện tất cả các nội dung dưới đây:

- Thời gian có hiệu lực của chứng thư số;
- Trạng thái chứng thư số qua danh sách chứng thư số thu hồi (CRL) được công bố tại thời điểm ký số hoặc bằng phương pháp kiểm tra trạng thái chứng thư số trực tuyến (OCSP) ở chế độ trực tuyến trong trường hợp tổ chức cung cấp dịch vụ chứng thực chữ ký số có cung cấp dịch vụ OCSP;

- Thuật toán mật mã trên chứng thư số;
- Mục đích, phạm vi sử dụng của chứng thư số.

d) Hiệu lực của chứng thư số khi đáp ứng tất cả các tiêu chí sau:

- Thời gian trên chứng thư số còn hiệu lực tại thời điểm ký số;
- Các thuật toán mật mã trên chứng thư số tuân thủ theo quy định về quy chuẩn, tiêu chuẩn kỹ thuật bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số đang có hiệu lực;

- Trạng thái của chứng thư số còn hoạt động tại thời điểm ký số;
- Chứng thư số được sử dụng đúng mục đích, phạm vi sử dụng.

đ) Cho phép kiểm tra tính toàn vẹn của thông điệp dữ liệu ký số:

- Giải mã chữ ký số trên thông điệp dữ liệu để có thông tin về mã băm;
 - Sử dụng thuật toán hàm băm an toàn đã tạo ra mã băm trên chữ ký số để thực hiện tạo mã băm cho thông điệp dữ liệu;
 - So sánh sự trùng khớp của hai mã băm để kiểm tra tính toàn vẹn của thông điệp dữ liệu ký số.
- e) Chữ ký số trên thông điệp dữ liệu là hợp lệ khi:
- Việc kiểm tra, xác thực được đúng thông tin người ký số;
 - Chứng thư số của người ký số tại thời điểm ký còn hiệu lực;
 - Xác minh chữ ký số trên thông điệp dữ liệu đúng với khóa bí mật tương ứng với khóa công khai trên chứng thư số và thông điệp dữ liệu đảm bảo tính toàn vẹn.

2. Chức năng lưu trữ và hủy bỏ các thông tin sau kèm theo thông điệp dữ liệu ký số:

- a) Các chứng thư số tương ứng với các chữ ký số trên thông điệp dữ liệu ký số được gửi đến;
- b) Các danh sách chứng thư số thu hồi tại thời điểm ký của tổ chức cung cấp chứng thực chữ ký số tương ứng với chữ ký số trên thông điệp dữ liệu được gửi đến;
- c) Quy chế chứng thực của các tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp phát chứng thư số tương ứng với các chữ ký số trên thông điệp dữ liệu được gửi đến;
- d) Kết quả kiểm tra trạng thái chứng thư số tương ứng với chữ ký số trên thông điệp dữ liệu được gửi đến.

3. Chức năng thay đổi (thêm, bớt) chứng thư số của tổ chức cung cấp dịch vụ chứng thực chữ ký số.

4. Chức năng thông báo (bằng chữ/bằng ký hiệu) việc kiểm tra tính hợp lệ của chữ ký số là hợp lệ hay không hợp lệ.

Chương III

ĐIỀU KHOẢN THI HÀNH

Điều 8. Tổ chức thực hiện

1. Trung tâm Chứng thực điện tử quốc gia có trách nhiệm hướng dẫn thực hiện các nội dung của Thông tư này.

2. Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng, tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng của cơ quan, tổ chức công bố các