

Số: **1911** /QĐ-BTTTT

Hà Nội, ngày **11** tháng 8 năm 2016

**QUYẾT ĐỊNH**

**Về việc ban hành Kế hoạch chuyển đổi chuẩn hàm băm an toàn của các tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng**

**BỘ TRƯỞNG BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

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;

Căn cứ Nghị định số 132/2013/NĐ-CP ngày 16 tháng 10 năm 2013 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Căn cứ Thông tư số 06/2015/TT-BTTTT ngày 23 tháng 3 năm 2015 của Bộ trưởng Bộ Thông tin và Truyền thông quy định danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số;

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

**QUYẾT ĐỊNH:**

**Điều 1.** Ban hành kèm theo Quyết định này “Kế hoạch chuyển đổi chuẩn hàm băm an toàn của các tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng”.

**Điều 2.** Quyết định này có hiệu lực thi hành kể từ ngày ký.

**Điều 3.** Chánh Văn phòng, Giám đốc Trung tâm Chứng thực điện tử quốc gia, thủ trưởng các đơn vị có liên quan, các tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng và các cơ quan, tổ chức ứng dụng chữ ký số công cộng chịu trách nhiệm thi hành Quyết định này. /.

**Nơi nhận:**

- Như Điều 3;
- Bộ trưởng và các Thứ trưởng;
- Các đơn vị thuộc Bộ;
- Lưu: VT, NEAC<sup>(60)</sup>.

**KT. BỘ TRƯỞNG**  
**THỨ TRƯỞNG**



**Nguyễn Thành Hưng**

**KẾ HOẠCH**  
**CHUYỂN ĐỔI CHUẨN HÀM BẮM AN TOÀN CỦA CÁC TỔ CHỨC**  
**CUNG CẤP DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG**  
*(Ban hành kèm theo Quyết định số 144/QĐ-BTTTT ngày 11 tháng 8 năm 2016*  
*của Bộ trưởng Bộ Thông tin và Truyền thông)*

Thực hiện Thông tư số 06/2015/TT-BTTTT ngày 23 tháng 3 năm 2015 của Bộ trưởng Bộ Thông tin và Truyền thông quy định danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số, Bộ Thông tin và Truyền thông tổ chức thực hiện việc chuyển đổi chuẩn hàm băm an toàn của các tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng (sau đây gọi tắt là các CA công cộng), cụ thể như sau:

**1. MỤC ĐÍCH, YÊU CẦU**

a) Thực hiện quy định về hàm băm an toàn trong Thông tư số 06/2015/TT-BTTTT ngày 23 tháng 3 năm 2015 của Bộ trưởng Bộ Thông tin và Truyền thông quy định danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số.

b) Nâng cao chất lượng, đảm bảo an toàn cho chữ ký số và dịch vụ chứng thực chữ ký số do các CA công cộng cung cấp.

c) Giảm thiểu tác động đến việc sử dụng chữ ký số, dịch vụ chứng thực chữ ký số của khách hàng đang sử dụng chữ ký số do các CA công cộng cung cấp.

d) Đảm bảo tính khả thi về thời gian và kỹ thuật cho các CA công cộng.

**2. MỤC TIÊU CHUYỂN ĐỔI**

a) Các CA công cộng hoàn thành việc chuyển đổi chứng thư số sử dụng chuẩn hàm băm an toàn SHA-1 sang SHA-256 trước ngày 31 tháng 12 năm 2016.

b) Toàn bộ khách hàng của các CA công cộng hoàn thành việc chuyển đổi chứng thư số sử dụng chuẩn hàm băm an toàn từ SHA-1 sang SHA-256 trước ngày 31 tháng 12 năm 2017.

### **3. KẾ HOẠCH CHUYỂN ĐỔI**

**3.1. Nhóm 1: Các CA công cộng hết hạn Giấy phép cung cấp dịch vụ chứng thực chữ ký số công cộng trong năm 2016**, bao gồm: CK-CA, Safe-CA, Newtel-CA, SmartSign.

- Các CA công cộng thuộc Nhóm 1 được cấp chứng thư số mới sử dụng chuẩn hàm băm an toàn SHA-256 sau khi được Bộ Thông tin và Truyền thông cấp Giấy phép cung cấp dịch vụ chứng thực chữ ký số mới *(nếu được cấp Giấy phép mới)*.

- Trong vòng 90 ngày kể từ khi được cấp chứng thư số mới sử dụng chuẩn hàm băm an toàn SHA-256, các CA công cộng Nhóm 1 chấm dứt việc cấp chứng thư số cho khách hàng *(bao gồm: cấp mới, gia hạn, cấp đổi chứng thư số)* sử dụng chuẩn hàm băm an toàn SHA-1.

- Chứng thư số hiện tại sử dụng chuẩn hàm băm an toàn SHA-1 của các CA công cộng thuộc Nhóm 1 được duy trì hiệu lực *(nếu còn hiệu lực)* để xác thực chữ ký số của khách hàng đến ngày 31 tháng 5 năm 2017, sau đó sẽ bị thu hồi.

- Quy trình, thủ tục cấp chứng thư số mới cho các CA công cộng thuộc Nhóm 1, sau khi được Bộ Thông tin và Truyền thông cấp Giấy phép mới, tuân theo các quy định tại 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, Thông tư số 37/2009/TT-BTTTT ngày 14 tháng 12 năm 2009 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về hồ sơ và thủ tục liên quan đến cấp phép, đăng ký, công nhận các tổ chức cung cấp dịch vụ chứng thực chữ ký số và Thông tư số 08/2011/TT-BTTTT ngày 31 tháng 3 năm 2011 của Bộ trưởng Bộ Thông tin và Truyền thông sửa đổi, bổ sung một số điều của Thông tư số 37/2009/TT-BTTTT.

**3.2. Nhóm 2: Các CA đã được cấp mới Giấy phép cung cấp dịch vụ chứng thực chữ ký số công cộng trong năm 2015**, bao gồm: BKAV-CA, CA2, Viettel-CA, FPT-CA.

- Các CA công cộng thuộc Nhóm 2 được cấp chứng thư số mới sử dụng chuẩn hàm băm an toàn SHA-256 trong Quý III năm 2016.

- Trong vòng 90 ngày kể từ khi được cấp chứng thư số mới sử dụng chuẩn hàm băm an toàn SHA-256, các CA công cộng Nhóm 2 chấm dứt việc cấp chứng thư số cho khách hàng *(bao gồm: cấp mới, gia hạn, cấp đổi chứng thư số)* sử dụng chuẩn hàm băm an toàn SHA-1.

- Chứng thư số hiện tại sử dụng chuẩn hàm băm an toàn SHA-1 của các CA công cộng thuộc Nhóm 2 được duy trì hiệu lực để xác thực chữ ký số của khách hàng đến ngày 31 tháng 12 năm 2017, sau đó sẽ bị thu hồi.

- Quy trình, thủ tục cấp chứng thư số mới cho các CA công cộng thuộc Nhóm 2 tuân theo các quy định tại 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, Thông tư số 37/2009/TT-BTTTT ngày 14 tháng 12 năm 2009 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về hồ sơ và thủ tục liên quan đến cấp phép, đăng ký, công nhận các tổ chức cung cấp dịch vụ chứng thực chữ ký số và Thông tư số 08/2011/TT-BTTTT ngày 31 tháng 3 năm 2011 của Bộ trưởng Bộ Thông tin và Truyền thông sửa đổi, bổ sung một số điều của Thông tư số 37/2009/TT-BTTTT.

**3.3. Nhóm 3: Các CA công cộng đã hết hạn Giấy phép cung cấp dịch vụ chứng thực chữ ký số công cộng, đang trong quá trình xin cấp Giấy phép mới, bao gồm: VNPT-CA.**

- Các CA công cộng thuộc Nhóm 3 được cấp chứng thư số mới sử dụng chuẩn hàm băm an toàn SHA-256 sau khi được Bộ Thông tin và Truyền thông cấp Giấy phép cung cấp dịch vụ chứng thực chữ ký số mới (nếu được cấp Giấy phép mới).

- Trong vòng 90 ngày kể từ khi được cấp chứng thư số mới sử dụng chuẩn hàm băm an toàn SHA-256, các CA công cộng Nhóm 3 chấm dứt việc cấp chứng thư số cho khách hàng (bao gồm: cấp mới, gia hạn, cấp đổi chứng thư số) sử dụng chuẩn hàm băm an toàn SHA-1.

- Chứng thư số hiện tại của các CA công cộng thuộc Nhóm 3 (sử dụng chuẩn hàm băm an toàn SHA-1) được duy trì hiệu lực để xác thực chữ ký số của khách hàng đến hết ngày 31 tháng 12 năm 2017, sau đó sẽ bị thu hồi.

- Quy trình, thủ tục cấp chứng thư số mới cho các CA công cộng thuộc Nhóm 3, sau khi được Bộ Thông tin và Truyền thông cấp Giấy phép mới, tuân theo các quy định tại 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, Thông tư số 37/2009/TT-BTTTT ngày 14 tháng 12 năm 2009 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về hồ sơ và thủ tục liên quan đến cấp phép, đăng ký, công nhận các tổ chức cung cấp dịch vụ chứng thực chữ ký số và Thông tư số 08/2011/TT-BTTTT ngày 31 tháng 3 năm 2011 của Bộ trưởng Bộ Thông tin và Truyền thông sửa đổi, bổ sung một số điều của Thông tư số 37/2009/TT-BTTTT.

## **4. TỔ CHỨC THỰC HIỆN**

### **4.1. Trung tâm Chứng thực điện tử quốc gia**

- Chuẩn bị sẵn sàng hệ thống chứng thực chữ ký số quốc gia (RootCA) để cấp chứng thư số mới sử dụng chuẩn hàm băm an toàn SHA-256 cho các CA công cộng.

- Tổ chức cấp chứng thư số sử dụng chuẩn hàm băm an toàn SHA-256 cho các CA công cộng đủ điều kiện.

- Hỗ trợ các CA công cộng trong quá trình chuyển đổi chuẩn hàm băm an toàn từ SHA-1 sang SHA-256.

- Thông báo đến các cơ quan, tổ chức ứng dụng chữ ký số như: Tổng cục Thuế, Tổng cục Hải quan, Bảo hiểm xã hội Việt Nam,... về việc chuyển đổi chuẩn hàm băm an toàn từ SHA-1 sang SHA-256 để các cơ quan, tổ chức chuẩn bị việc nâng cấp hệ thống, đáp ứng chuẩn hàm băm an toàn SHA-256.

- Định kỳ hàng quý, báo cáo Bộ Thông tin và Truyền thông kết quả việc chuyển đổi chuẩn hàm băm an toàn của các CA công cộng, đề xuất các giải pháp hỗ trợ các CA công cộng khi cần thiết, đồng thời, gửi thông tin đến các đơn vị cung cấp ứng dụng sử dụng chữ ký số công cộng để biết và phối hợp thực hiện.

### **4.2. Các CA công cộng thuộc Nhóm 1**

- Khẩn trương nộp, hoàn thiện hồ sơ xin cấp Giấy phép cung cấp dịch vụ chứng thực chữ ký số công cộng mới theo các quy định của pháp luật.

- Nộp hồ sơ xin cấp chứng thư số mới ngay sau khi được cấp Giấy phép mới (nếu được cấp Giấy phép mới).

- Chuẩn bị hệ thống kỹ thuật (hệ thống chứng thực chữ ký số, usb token,...) đáp ứng chuẩn hàm băm an toàn SHA-256.

- Thông báo cho khách hàng về việc chuyển đổi chuẩn hàm băm an toàn để có sự chuẩn bị. Thực hiện việc chuyển đổi chứng thư số cho khách hàng sử dụng chuẩn hàm băm an toàn SHA-256, hoàn thành trước ngày 31 tháng 5 năm 2017.

### **4.3. Các CA công cộng thuộc Nhóm 2**

- Nộp hồ sơ xin cấp chứng thư số mới theo quy định của pháp luật.

- Chuẩn bị hệ thống kỹ thuật (hệ thống chứng thực chữ ký số, usb token,...) đáp ứng chuẩn hàm băm an toàn SHA-256.

- Thông báo cho khách hàng về việc chuyển đổi chuẩn hàm băm an toàn để có sự chuẩn bị. Thực hiện việc chuyển đổi chứng thư số cho khách hàng theo chuẩn hàm băm an toàn SHA-256, hoàn thành trước ngày 31 tháng 12 năm 2017.

#### **4.4. Các CA công cộng thuộc Nhóm 3**

- Khẩn trương hoàn thiện, bổ sung hồ sơ xin cấp Giấy phép cung cấp dịch vụ chứng thực chữ ký số công cộng mới theo các quy định của pháp luật, theo yêu cầu của Bộ Thông tin và Truyền thông và các cơ quan liên quan.

- Nộp hồ sơ xin cấp chứng thư số mới ngay sau khi được cấp Giấy phép mới (nếu được cấp Giấy phép mới).

- Chuẩn bị hệ thống kỹ thuật (hệ thống chứng thực chữ ký số, usb token,...) đáp ứng việc chuyển đổi chuẩn hàm băm an toàn từ SHA-1 sang SHA-256.

- Thông báo cho khách hàng về việc chuyển đổi chuẩn hàm băm an toàn để có sự chuẩn bị. Thực hiện việc chuyển đổi chứng thư số cho khách hàng sử dụng chuẩn hàm băm an toàn SHA-256, hoàn thành trước ngày 31 tháng 12 năm 2017.

#### **4.4. Tổng cục Thuế, Tổng cục Hải quan, Bảo hiểm xã hội Việt Nam và các đơn vị có ứng dụng sử dụng chữ ký số của các CA công cộng**

- Chuẩn bị hệ thống để phối hợp kiểm thử với các CA công cộng, đảm bảo hệ thống sẵn sàng tiếp nhận, xác thực chữ ký số của các CA công cộng sử dụng chuẩn hàm băm an toàn SHA-256 trước ngày 31 tháng 12 năm 2016.

- Thông báo bằng văn bản tới các CA công cộng về việc hệ thống ứng dụng của đơn vị mình sẵn sàng tiếp nhận và xác thực chữ ký số của các CA công cộng sử dụng chuẩn hàm băm an toàn SHA-256.

- Thông báo cho các CA công cộng, các ngân hàng, các tổ chức T-VAN và các đơn vị liên quan về việc chuyển đổi chuẩn hàm băm an toàn để các đơn vị biết và hướng dẫn, hỗ trợ khách hàng trong quá trình sử dụng chữ ký số.

- Thực hiện hỗ trợ các CA công cộng và khách hàng sử dụng chữ ký số trong quá trình chuyển đổi chuẩn hàm băm an toàn từ SHA-1 sang SHA-256 đến hết ngày 31 tháng 12 năm 2017./.

**KT. BỘ TRƯỞNG  
THỨ TRƯỞNG**



**Nguyễn Thành Hưng**