

	VIETTEL AI RACE	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Cổng kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

*Căn cứ Luật giao dịch điện tử ngày 22 tháng 06 năm 2023;*

*Căn cứ Nghị định số 23/2025/NĐ-CP ngày 21 tháng 02 năm 2025 của Chính phủ quy định về chữ ký điện tử và dịch vụ tin cậy;*

*Căn cứ Nghị định số 55/2025/NĐ-CP ngày 02 tháng 3 năm 2025 của Chính phủ quy định chức năng, nhiệm vụ và cơ cấu tổ chức của Bộ Khoa học và Công nghệ;*

**Theo đề nghị của Vụ trưởng Vụ Pháp chế và Giám đốc Trung tâm Chứng thực điện tử quốc gia;**

Bộ trưởng Bộ Khoa học và Công nghệ ban hành Thông tư quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Cổng kết nối dịch vụ chứng thực chữ ký số công cộng.

## 1. QUY ĐỊNH CHUNG

### 1.1. Phạm vi điều chỉnh

Thông tư này quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Cổng kết nối dịch vụ chứng thực chữ ký số công cộng.

### 1.2 . Đối tượng áp dụng

Thông tư này áp dụng đối với tổ chức, cá nhân sử dụng phần mềm ký số, phần mềm kiểm tra chữ ký số; các tổ chức, cá nhân phát triển phần mềm ký số, phần mềm kiểm tra chữ ký số; **các tổ chức cung cấp dịch vụ chứng thực chữ ký số; các tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử chuyên dùng đảm bảo an toàn; các tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử nước ngoài được công nhận tại Việt Nam; chủ quản các hệ thống thông tin phục vụ giao dịch điện tử có sử dụng chữ ký số** và các tổ chức, cá nhân có liên quan khác.

	<b>VIETTEL AI RACE</b>	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Công kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

### 1.3. Giải thích từ ngữ

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

- “Cặp khóa bất đối xứng” là khóa công khai và khóa bí mật tương ứng.
- “Khóa bí mật” là thành phần của cặp khóa bất đối xứng được sử dụng để ký thông điệp dữ liệu.
- “Khóa công khai” là thành phần của cặp khóa bất đối xứng được sử dụng để xác thực chữ ký số trên thông điệp dữ liệu.
- “Chủ thẻ ký” là cá nhân hoặc tổ chức sở hữu chứng thư chữ ký số và sử dụng khóa bí mật tương ứng để thực hiện ký số trên thông điệp dữ liệu.
- “Chứng thư **chữ ký số**” 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 về khóa công khai của một cá nhân, tổ chức từ đó xác nhận cá nhân, tổ chức là **chủ thẻ** ký thông qua việc sử dụng khóa bí mật tương ứng.
- “Phần mềm ký số” là chương trình độc lập hoặc một thành phần (module) phần mềm hoặc giải pháp có chức năng ký số vào thông điệp dữ liệu.
- “Phần mềm kiểm tra chữ ký số” là chương trình 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 đã ký.
- “Đường dẫn **tin cậy** của chứng thư **chữ ký số**” là thông tin đường dẫn trên chứng thư chữ ký số xác thực tổ chức cung cấp dịch vụ chứng thực chữ ký số đã cấp phát ra chứng thư **chữ ký số** đó.

## 2. Yêu cầu kỹ thuật đối với chức năng phần mềm ký số, phần mềm kiểm tra chữ ký số

### 2.1 Yêu cầu chung

Tuân thủ các yêu cầu và tiêu chuẩn kỹ thuật về chữ ký số trên thông điệp dữ liệu tại Phụ lục I ban hành kèm theo Thông tư này.

	VIETTEL AI RACE	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Cổng kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

## 2.2 Yêu cầu về chức năng

- Chức năng xác thực chủ thẻ ký và ký số:

- + Kiểm tra được thông tin chủ thẻ ký trên chứng thư chữ ký số;
- + Cho phép chủ thẻ ký sử dụng khóa bí mật để thực hiện việc ký số vào thông điệp dữ liệu. Khoá bí mật lưu trong thiết bị được chủ thẻ ký sử dụng để ký số phải tuân thủ các yêu cầu và tiêu chuẩn kỹ thuật tại Phụ lục I ban hành kèm theo Thông tư này;
- + Cho phép chuyển đổi định dạng thông điệp dữ liệu thành các định dạng được nêu tại Phụ lục I ban hành kèm theo Thông tư này;
- + Gắn kèm chữ ký số và chứng thư chữ ký số vào thông điệp dữ liệu sau khi ký số;
- + Hỗ trợ cài đặt, tích hợp chứng thư chữ ký số của Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia và chứng thư chữ ký số thuộc Danh sách tin cậy chứng thư chữ ký điện tử nước ngoài được công nhận tại Việt Nam;
- + Đáp ứng các giao thức gửi nhận thông điệp dữ liệu của phần mềm ký số theo các yêu cầu và tiêu chuẩn tại Phụ lục I ban hành kèm theo Thông tư này.

- Chức năng kiểm tra hiệu lực của chứng thư chữ ký số:

- + Thông tin trong chứng thư chữ ký số được định danh theo quy định pháp luật về định danh và xác thực điện tử;
- + Chứng thư chữ ký số của chủ thẻ ký phải được kiểm tra theo đường dẫn tin cậy của chứng thư chữ ký số đó và phải liên kết đến chứng thư chữ ký số gốc của Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia hoặc thuộc Danh sách tin cậy chứng thư chữ ký điện tử nước ngoài được công nhận tại Việt Nam;
- + Chứng thư chữ ký số phải có hiệu lực tại thời điểm ký số và đáp ứng các tiêu chí tại Phụ lục II ban hành kèm theo Thông tư này.

- Chức năng kết nối đến Cổng kết nối dịch vụ chứng thực chữ ký số công cộng: Hướng dẫn kết nối được quy định tại **Chương III** Thông tư này.

	<b>VIETTEL AI RACE</b>	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Công kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

- Chức năng lưu trữ và hủy bỏ các thông tin kèm theo thông điệp dữ liệu ký số, bao gồm:

- + Chứng thư chữ ký số tương ứng với khóa bí mật mà **chủ thẻ** ký sử dụng để ký thông điệp dữ liệu tại thời điểm ký số;

- + Danh sách chứng thư chữ ký số thu hồi tại thời điểm ký **trong chứng thư chữ ký số của chủ thẻ**;

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

- + Kết quả kiểm tra trạng thái chứng thư chữ ký số tương ứng với chữ ký số trên thông điệp dữ liệu đã ký.

- Chức năng thay đổi (thêm, bớt) chứng thư chữ ký số của cơ quan, tổ chức tạo lập cấp, phát hành chứng thư chữ ký số:

Cho phép tích hợp và hiển thị đầy đủ các tổ chức cung cấp dịch vụ chứng thực chữ ký số và Danh sách tin cậy chứng thư chữ ký điện tử nước ngoài được công nhận tại Việt Nam.

- Chức năng thông báo bằng chữ hoặc ký hiệu cho **chủ thẻ** ký biết việc ký số vào thông điệp dữ liệu thành công hay không thành công, bao gồm việc:

- + **Hiển thị thông báo ký số thành công hoặc không thành công;**

- + Xem được thông điệp dữ liệu đã ký sau khi hoàn thành ký số;

- + Tải được thông điệp dữ liệu đã ký về thiết bị.

### 2.3 Yêu cầu chung

Tuân thủ các yêu cầu và tiêu chuẩn kỹ thuật về chữ ký số trên thông điệp dữ liệu tại Phụ lục I ban hành kèm theo Thông tư này.

### 2.4 Yêu cầu về chức năng

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

	VIETTEL AI RACE	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Công kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

+ Cho phép xác **thực** 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 chữ ký số;

+ Cho phép kiểm tra chứng thư chữ ký số của **chủ thẻ** ký theo đường dẫn tin cậy của chứng thư chữ ký số đó và phải **liên kết** đến Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia **hoặc** thuộc Danh sách tin cậy chứng thư chữ ký điện tử nước ngoài được công nhận tại Việt Nam;

+ Bảo đảm chứng thư chữ ký số phải có hiệu lực tại thời điểm ký số và đáp ứng các tiêu chí tại Phụ lục II ban hành kèm theo Thông tư này;

+ Cho phép kiểm tra tính toàn vẹn của thông điệp dữ liệu ký số **theo các bước sau:**

- Giải mã chữ ký số trên thông điệp dữ liệu để có thông tin về mã băm của thông điệp dữ liệu;

- 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.

+ Đảm bảo tính hợp lệ của chữ ký số trên thông điệp dữ liệu đã ký theo các tiêu chí tại Phụ lục II ban hành kèm theo Thông tư này;

+ Hỗ trợ cài đặt, tích hợp chứng thư chữ ký số của Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia và chứng thư chữ ký số thuộc danh sách tin cậy chứng thư chữ ký điện tử nước ngoài được công nhận tại Việt Nam;

+ Đáp ứng các giao thức gửi nhận thông điệp dữ liệu của phần mềm ký số theo tiêu chuẩn tại Phụ lục I ban hành kèm theo Thông tư này.

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

	<b>VIETTEL AI RACE</b>	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Cổng kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

- + Chứng thư chữ ký số tương ứng với chữ ký số trên thông điệp dữ liệu đã ký;
- + Danh sách chứng thư chữ ký số thu hồi tại thời điểm ký **được thể hiện** trong chứng thư chữ ký số đính kèm thông điệp dữ liệu đã ký;
- + Quy chế chứng thực của các tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp phát chứng thư chữ ký số tương ứng với các chữ ký số trên thông điệp dữ liệu **đã ký**;
- + Kết quả kiểm tra trạng thái chứng thư chữ ký số tương ứng với chữ ký số trên thông điệp dữ liệu **đã ký**.
- Chức năng thay đổi (thêm, bớt) chứng thư chữ ký số của cơ quan, tổ chức tạo lập, cấp, phát hành chứng thư chữ ký số.
- Chức năng thông báo bằng chữ hoặc ký hiệu việc kiểm tra tính hợp lệ của chữ ký số là hợp lệ hay không hợp lệ:
  - + **Hiển thị thông báo chữ ký số** trên thông điệp dữ liệu đã ký hợp lệ hay không hợp lệ;
  - + **Hiển thị** các thông tin về chữ ký số và chứng thư chữ ký số trên thông điệp dữ liệu đã ký, với tối thiểu các trường thông tin sau: thông tin về cơ quan, tổ chức tạo lập, cấp, phát hành chứng thư chữ ký số; thông tin về chủ thẻ ký; thông tin về thời điểm ký số hoặc dấu thời gian (nếu có); tính toàn vẹn của thông điệp dữ liệu đã ký; tính hợp lệ của chữ ký số tại thời điểm ký.

### 3. CỔNG KẾT NỐI DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG

#### 3.1 Cổng kết nối dịch vụ chứng thực chữ ký số công cộng

Cổng kết nối dịch vụ chứng thực chữ ký số công cộng là hệ thống thông tin phục vụ kết nối dịch vụ chứng thực chữ ký số công cộng với các hệ thống thông tin phục vụ giao dịch điện tử sử dụng chữ ký số để bảo đảm tính xác thực, tính toàn vẹn và tính chống chối bỏ của thông điệp dữ liệu.

	<b>VIETTEL AI RACE</b>	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Cổng kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

### 3.2 Kết nối đến Cổng kết nối dịch vụ chứng thực chữ ký số công cộng

- Các tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng kết nối đến Cổng kết nối dịch vụ chứng thực chữ ký số công cộng, cụ thể:

+ Thực hiện theo Hướng dẫn kết nối tại Phụ lục III ban hành kèm theo Thông tư này;

+ Cung cấp các đặc tả, thông số kỹ thuật và thông tin phục vụ kết nối cho Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia;

+ Cập nhật các thông số kỹ thuật hoặc thông tin phục vụ kết nối khi có thay đổi cho Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia.

- Các hệ thống thông tin phục vụ giao dịch điện tử sử dụng chữ ký số tích hợp với Cổng kết nối dịch vụ chứng thực chữ ký số công cộng để bảo đảm tính xác thực, tính toàn vẹn và tính chống chối bỏ của thông điệp dữ liệu, cụ thể:

+ Thực hiện theo Hướng dẫn kết nối tại Phụ lục III ban hành kèm theo Thông tư này;

+ Bảo đảm chức năng ký số của hệ thống thông tin phục vụ giao dịch điện tử sử dụng chữ ký số đáp ứng các quy định tại Điều 5 Thông tư này;

+ Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia cung cấp các đặc tả, thông số kỹ thuật và thông tin phục vụ việc kết nối đến Cổng kết nối dịch vụ chứng thực chữ ký số công cộng.

- Đầu mối hỗ trợ, hướng dẫn kết nối đến Cổng kết nối dịch vụ chứng thực chữ ký số công cộng: Trung tâm Chứng thực điện tử quốc gia, Bộ Khoa học và Công nghệ.

	<b>VIETTEL AI RACE</b>	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Công kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

## 4. ĐIỀU KHOẢN THI HÀNH

### 4.1 Tổ chức thực hiện

- Trung tâm Chứng thực điện tử quốc gia có trách nhiệm hướng dẫn thực hiện các nội dung của Thông tư này và công bố thông tin theo quy định tại điểm c khoản 2 Điều 9 Thông tư này.

- Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng, tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử chuyên dùng đảm bảo an toàn, **Tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử nước ngoài được công nhận tại Việt Nam có trách nhiệm** công bố các đặc tả kỹ thuật (tài liệu và bộ công cụ), chứng thư chữ ký số liên quan đến tổ chức cung cấp dịch vụ chứng thực chữ ký số và các tiêu chuẩn chữ ký số trên trang tin điện tử của tổ chức cung cấp dịch vụ chứng thực chữ ký số đó.

- Tổ chức, cá nhân phát triển, sử dụng **phần mềm ký số, phần mềm kiểm tra chữ ký số** có trách nhiệm tuân thủ các quy định về yêu cầu kỹ thuật, hướng dẫn sử dụng đối với phần mềm ký số, phần mềm kiểm tra chữ ký số.

### 4.2 Hiệu lực thi hành

- Thông tư này có hiệu lực thi hành kể từ ngày tháng năm .
- Chánh Văn phòng, Giám đốc Trung tâm Chứng thực điện tử quốc gia, Thủ trưởng các cơ quan, đơn vị thuộc Bộ, Giám đốc Sở Khoa học và Công nghệ các tỉnh, thành phố trực thuộc Trung ương, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này.
- Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, cơ quan, tổ chức, cá nhân phản ánh kịp thời về Bộ Khoa học và Công nghệ (Trung tâm Chứng thực điện tử quốc gia) để xem xét, giải quyết./.

	VIETTEL AI RACE	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Công kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

## Phụ lục I

### **DANH MỤC TIÊU CHUẨN KỸ THUẬT VỀ CHỮ KÝ SỐ TRÊN THÔNG ĐIỆP DỮ LIỆU DÙNG CHO PHẦN MỀM KÝ SỐ VÀ PHẦN MỀM KIỂM TRA CHỮ KÝ SỐ**

*(Ban hành kèm theo Thông tư số /2025/TT-BKHCN ngày tháng năm 2025 của Bộ trưởng Bộ Khoa học và Công nghệ)*

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
<b>Tiêu chuẩn về định dạng thông điệp dữ liệu</b>				
11	Bộ ký tự và mã hóa	ASCII	American Standard Code for Information Interchange	Khuyến nghị áp dụng
12	Bộ ký tự và mã hóa cho tiếng Việt	TCVN 6909:2001	TCVN 6909:2001 “Công nghệ thông tin-Bộ mã ký tự tiếng Việt 16-bit”	Bắt buộc áp dụng
13	Trình diễn bộ ký tự	UTF-8	8-bit Universal Character Set (UCS)/ Unicode Transformation Format	Khuyến nghị áp dụng
14	Ngôn ngữ định dạng thông điệp dữ liệu	XML v1.0 (5th Edition)	Extensible Markup Language version 1.0 (5th Edition)	Khuyến nghị áp dụng một trong hai tiêu chuẩn
		XML v1.1 (2nd Edition)	Extensible Markup Language version 1.1	

	VIETTEL AI RACE	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Công kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

15	<i>Định nghĩa các lược đồ trong tài liệu XML</i>	<i>XML Schema version 1.1</i>	<i>XML Schema version 1.1</i>	<i>Khuyến nghị áp dụng</i>
16	<i>Trao đổi dữ liệu đặc tả tài liệu XML</i>	<i>XML v2.4.2</i>	<i>XML Metadata Interchange version 2.4.2</i>	<i>Khuyến nghị áp dụng</i>
77	<i>Quản lý tài liệu - Định dạng tài liệu di động</i>	<i>ISO 32000-1:2008</i>	<i>Document management - Portable document format</i>	<i>Khuyến nghị áp dụng</i>
88	<i>Định dạng trao đổi dữ liệu theo ký hiệu đối tượng Javascript</i>	<i>RFC7159</i>	<i>The JavaScript Object Notation (JSON) Data Interchange Format</i>	<i>Khuyến nghị áp dụng</i>
<i>Tiêu chuẩn về ký số, kiểm tra chữ ký số</i>				
21	<i>Tiêu chuẩn về ký số trên thiết bị quản lý khóa bí mật, phần mềm ký số, tạo chữ ký số, chứng thư số, phần mềm kiểm tra chữ ký số.</i>			
21.1	<i>Thuật toán mã hóa</i>	<i>TCVN 7816:2007</i>	<i>Công nghệ thông tin. Kỹ thuật mật mã - thuật toán mã dữ liệu AES</i>	<i>Khuyến nghị áp dụng</i>
		<i>NIST 800-67</i>	<i>Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher</i>	<i>Khuyến nghị áp dụng</i>

	<b>VIETTEL AI RACE</b>	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Công kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

		<b>PKCS#1</b> <i>RSA Cryptography Standard (Phiên bản 2.1 trở lên)</i> <i>Áp dụng, sử dụng lược đồ RSAES-OAEP để mã hóa</i> <i>Độ dài khóa tối thiểu là 2048 bit</i>	<i>Khuyến nghị áp dụng</i>
		<b>ECC</b> <i>Elliptic Curve Cryptography</i>	<i>Khuyến nghị áp dụng</i>
		<b>TCVN 7635:2007</b> <i>Các kỹ thuật mật mã - Chữ ký số</i>	<ul style="list-style-type: none"> <li>- Áp dụng một trong ba tiêu chuẩn.</li> </ul>
		<b>PKCS#1</b> <i>RSA Cryptography Standard</i>	<ul style="list-style-type: none"> <li>- Đối với tiêu chuẩn TCVN 7635:2007 và PKCS#1:</li> <li>+ Phiên bản 2.1</li> <li>+ Áp dụng lược đồ RSAES-OAEP để mã hóa và RSASSA-PSS để ký.</li> <li>+ Độ dài khóa tối thiểu là 2048 bit</li> </ul>
		<b>ANSI X9.62-2005</b> <i>Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)</i>	<ul style="list-style-type: none"> <li>- Đối với tiêu chuẩn ECDSA: độ dài khóa tối thiểu là 256 bit</li> </ul>

	VIETTEL AI RACE	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Công kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

21.3	<i>Hàm băm an toàn</i>	<i>FIPS PUB 180-4</i>	<i>Secure Hash Algorithms</i>	<i>Áp dụng một trong các hàm băm sau:</i> <i>SHA-224,</i> <i>SHA-256,</i> <i>SHA-384,</i> <i>SHA-512,</i> <i>SHA-512/224,</i> <i>SHA-512/256,</i> <i>SHA3-224,</i> <i>SHA3-256,</i> <i>SHA3-384,</i> <i>SHA3-512,</i> <i>SHAKE128,</i> <i>SHAKE256</i>
		<i>FIPS PUB 202</i>	<i>SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions</i>	
21.4	<i>Cú pháp mã hóa và cách xử lý thông điệp dữ liệu định dạng XML</i>	<i>XML Encryption Syntax and Processing</i>	<i>XML Encryption Syntax and Processing</i>	<i>Bắt buộc áp dụng</i>
		<i>XML Signature Syntax and Processing</i>	<i>XML Signature Syntax and Processing</i>	<i>Bắt buộc áp dụng</i>
21.5	<i>Quản lý khóa công khai thông điệp dữ liệu định dạng XML</i>	<i>XKMS v2.0</i>	<i>XML Key Management Specification version 2.0</i>	<i>Bắt buộc áp dụng</i>
21.6	<i>Cú pháp thông điệp</i>	<i>PKCS#7 v1.5 (RFC 2315)</i>	<i>Cryptographic message syntax for file-based</i>	<i>Bắt buộc áp dụng</i>

	VIETTEL AI RACE	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Công kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

	<i>mật mã cho ký, mã hóa</i>		<i>signing and encrypting version 1.5</i>	
11.7	<i>Tiêu chuẩn về chữ ký điện tử nâng cao dành cho thông điệp dữ liệu định dạng PDF</i>	<i>ETSI EN 319 142-1</i>	<i>Electronic Signatures and Infrastructures (ESI) - PAdES digital signatures</i>	<i>Áp dụng một trong hai tiêu chuẩn PAdES hoặc CAdES</i>
11.8	<i>Tiêu chuẩn về chữ ký điện tử nâng cao dành cho thông điệp dữ liệu định dạng XML</i>	<i>ETSI TS 101 903</i>	<i>Electronic Signatures and Infrastructures (ESI) - XML Advanced Electronic Signatures (XAdES)</i>	<i>Áp dụng một trong hai tiêu chuẩn XAdES hoặc CAdES</i>
11.9	<i>Tiêu chuẩn về chữ ký điện tử nâng cao dành cho thông điệp dữ liệu định dạng JSON</i>	<i>RFC 7515</i>	<i>JSON Web Signature (JWS)</i>	<i>Bắt buộc áp dụng cho thông điệp dữ liệu định dạng JSON</i>
11.10	<i>Tiêu chuẩn về chữ ký điện tử nâng cao dành cho cú pháp tin nhắn mật mã</i>	<i>ETSI TS 101 733</i>	<i>Electronic Signatures and Infrastructures (ESI) - CMS Advanced Electronic Signatures (CAdES)</i>	<i>Khuyến nghị áp dụng</i>
.2	<i>Tiêu chuẩn về hệ thống, thiết bị lưu trữ và sử dụng khóa bí mật</i>			

	VIETTEL AI RACE	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Công kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

22.1	<i>Yêu cầu an toàn dành cho mô đun bảo mật phần cứng</i>	<i>FIPS PUB 140-2</i>	<i>Security Requirements for Cryptographic Modules</i>	<i>- Yêu cầu tối thiểu mức 3 (level 3)</i>
22.2	<i>Yêu cầu an toàn đối với thẻ Token và Smart card</i>	<i>FIPS PUB 140-2</i>	<i>Security Requirements for Cryptographic Modules</i>	<i>- Yêu cầu tối thiểu mức 2 (level 2)</i>
.2.3	<i>Yêu cầu về chính sách và an toàn cho các tổ chức cung cấp dịch vụ tin cậy: Các thành phần dịch vụ vận hành thiết bị tạo chữ ký số và hỗ trợ tạo chữ ký số AdES</i>	<i>ETSI TS 119 431-1</i>	<i>Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD/SCDev</i>	<i>Áp dụng cả bộ tiêu chuẩn 2 phần; Phiên bản V1.1.1 (12/2018)</i>
		<i>ETSI TS 119 431-2</i>	<i>Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation</i>	
.2.4	<i>Giao thức tạo chữ ký số từ xa</i>	<i>ETSI TS 119 432</i>	<i>Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation</i>	<i>Phiên bản V1.1.1 (03/2019)</i>

	VIETTEL AI RACE	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Công kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

.2.5	<i>Hệ thống tin cậy hỗ trợ ký số từ xa – Các yêu cầu chung</i>	EN 419241-1:2018	<i>Trustworthy Systems Supporting Server Signing - Part 1: General system security requirements</i>	
.2.6	<i>Hệ thống tin cậy hỗ trợ ký số từ xa – Yêu cầu và mục tiêu (hỗ trợ bảo vệ) của thiết bị tạo chữ ký số dành cho ký số từ xa</i>	EN 419241-2:2019	<i>Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing</i>	
.2.7	<i>Yêu cầu và mục tiêu (hỗ trợ bảo vệ) dành cho module bảo mật phần cứng của tổ chức cung cấp dịch vụ tin cậy – mô đun mã hóa dành cho các dịch vụ tin cậy</i>	EN 419221-5:2018	<i>Protection Profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services</i>	
33	<b>Tiêu chuẩn kiểm tra trạng thái chứng thư số</b>			
33.1	<i>Giao thức truyền, nhận</i>	RFC 2585	<i>Internet X.509 Public Key Infrastructure -</i>	<i>Áp dụng một hoặc cả hai giao</i>

	<b>VIETTEL AI RACE</b>	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Công kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

	<i>chứng thư chữ ký số và danh sách chứng thư chữ ký số bị thu hồi</i>		<i>Operational Protocols: FTP and HTTP</i>	<i>thức FTP và HTTP</i>
33.2	<i>Giao thức bảo mật tầng giao vận</i>	<i>RFC 8446</i>	<i>The Transport Layer Security (TLS) Protocol Version 1.3</i>	<i>Bắt buộc áp dụng tối thiểu</i>
33.3	<i>Giao thức cho kiểm tra trạng thái chứng thư chữ ký số trực tuyến</i>	<i>RFC 2560</i>	<i>X.509 Internet Public Key Infrastructure - On- line Certificate status protocol</i>	

	VIETTEL AI RACE	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Công kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

## Phụ lục II

### **DANH MỤC TIÊU CHÍ ĐÁNH GIÁ HIỆU LỰC CỦA CHỨNG THƯ CHỮ KÝ SỐ VÀ CHỮ KÝ SỐ HỢP LỆ TRONG PHẦN MỀM KÝ SỐ, PHẦN MỀM KIỂM TRA CHỮ KÝ SỐ**

*(Ban hành kèm theo Thông tư số /2025/TT-BKHCN ngày tháng năm 2025 của Bộ trưởng Bộ Khoa học và Công nghệ)*

<b>Số TT</b>	<b>Tiêu chí đánh giá</b>	<b>Hiệu lực/hợp lệ</b>	<b>Quy định áp dụng</b>
<b>1</b>	<b>Tính hiệu lực của chứng thư chữ ký số</b>		
1.1	Thời gian có hiệu lực của chứng thư số	Thời gian trên chứng thư chữ ký số còn hiệu lực tại thời điểm ký số	Bắt buộc áp dụng
1.2	Trạng thái chứng thư số qua danh sách chứng thư chữ ký số thu hồi (CRL) được công bố tại thời điểm ký số hoặc bằng phương pháp kiểm tra trạng thái chứng thư chữ ký 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	Trạng thái của chứng thư chữ ký số còn hoạt động tại thời điểm ký số	Bắt buộc áp dụng
1.3	Thuật toán mã trên chứng thư chữ ký số	Các thuật toán mã trên chứng thư chữ ký 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	Bắt buộc áp dụng

	VIETTEL AI RACE	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Công kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

		<i>chữ ký số đang có hiệu lực</i>	
1.4	<i>Mục đích, phạm vi sử dụng của chứng thư chữ ký số</i>	<i>Chứng thư chữ ký số được sử dụng đúng mục đích, phạm vi sử dụng</i>	<i>Bắt buộc áp dụng</i>
1.5	<i>Các tuyên bố khác của Tổ chức cung cấp dịch vụ chứng thực chữ ký số</i>	<i>Các tuyên bố khác không nằm ngoài phạm vi Quy chế chứng thực của Tổ chức cung cấp dịch vụ chứng thực chữ ký số</i>	<i>Khuyến nghị áp dụng</i>
<b>2</b>	<b>Tính hợp lệ của chữ ký số</b>		
2.1	<i>Thông tin về chủ thẻ ký</i>	<i>Kiểm tra, xác thực được đúng thông tin chủ thẻ ký số</i>	<i>Bắt buộc áp dụng</i>
2.2	<i>Cách thức tạo chữ ký số</i>	<i>Chữ ký số được tạo ra đúng bởi khóa bí mật tương ứng với khóa công khai trên chứng thư chữ ký số</i>	<i>Bắt buộc áp dụng</i>
2.3	<i>Chứng thư chữ ký số kèm theo thông điệp dữ liệu</i>	<i>Chứng thư chữ ký số có hiệu lực tại thời điểm ký</i>	<i>Bắt buộc áp dụng</i>
2.4	<i>Tính toàn vẹn của thông điệp dữ liệu</i>	<i>Mã băm có được từ việc băm thông điệp dữ liệu và mã băm có được khi giải mã chữ ký số trùng nhau</i>	<i>Bắt buộc áp dụng</i>

	<b>VIETTEL AI RACE</b>	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Công kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

	<b>VIETTEL AI RACE</b>	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Cổng kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

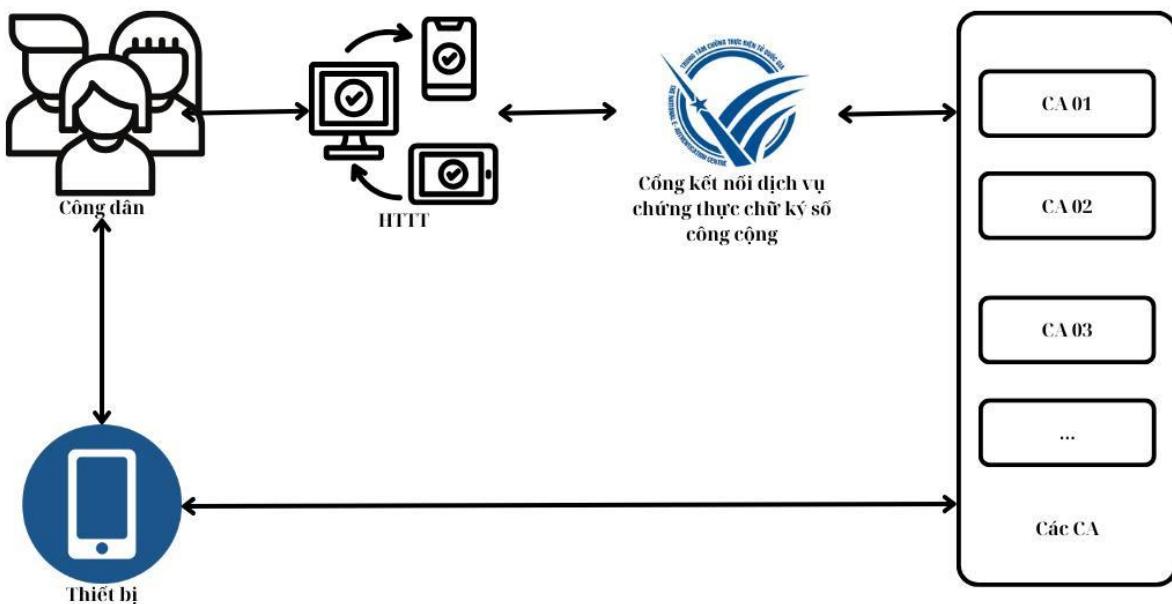
### **Phụ lục III**

## **HƯỚNG DẪN KẾT NỐI ĐẾN CỔNG KẾT NỐI DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG**

*(Ban hành kèm theo Thông tư số /2025/TT-BKHCN ngày tháng năm 2025 của Bộ trưởng Bộ Khoa học và Công nghệ)*

### **1. Mô hình kết nối**

Mô hình kết nối với Cổng kết nối dịch vụ chứng thực chữ ký số công cộng (sau đây gọi là Cổng eSign) được mô tả tại sơ đồ như sau:



**Chú thích:**

- HTTT: Hệ thống thông tin phục vụ giao dịch điện tử sử dụng chữ ký số.
- CA: Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.

### **2. Các thông tin hướng dẫn kết nối**

- a) Giao thức sử dụng để kết nối là API, phương thức kết nối là POST.
- b) Đường dẫn kết nối các API: <https://esign.neac.gov.vn>

	<b>VIETTEL AI RACE</b>	Public 257
	<b>Quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số và Công kết nối dịch vụ chứng thực chữ ký số công cộng</b>	Lần ban hành: 1

c) Thông tin Công eSign cung cấp cho các HTTT gồm: sp\_id và sp\_password hoặc token, trong đó:

- sp\_id: Mã xác thực được cấp cho HTTT.
- sp\_password: Mật khẩu kết nối được cấp cho HTTT tương ứng với sp\_id.
- token: Thông tin xác thực được cấp cho HTTT.