

**TẬP ĐOÀN CÔNG NGHIỆP VIỄN THÔNG QUÂN ĐỘI**

**TÀI LIỆU ĐẶC TẢ KẾT NỐI API**

**HỆ THỐNG CHỮ KÝ SỐ CLOUD CA**

**Phiên bản tài liệu: v1.0**

**Hà Nội, 04/2022**

**MỤC LỤC**

[1 GIỚI THIỆU 3](#_Toc127951697)

[1.1 Mục đích tài liệu 3](#_Toc127951698)

[1.2 Thuật ngữ 3](#_Toc127951699)

[1.3 Mô tả tài liệu 3](#_Toc127951700)

[2 CÁC LUỒNG XỬ LÝ GIAO TIẾP 4](#_Toc127951701)

[2.1 Nghiệp vụ ký điện tử 4](#_Toc127951702)

[3 ĐẶC TẢ GIAO TIẾP KÝ ĐỒNG BỘ 5](#_Toc127951703)

[3.1 Các loại giao dịch 5](#_Toc127951704)

[3.2 Đặc tả chi tiết các giao dịch 5](#_Toc127951705)

[3.2.1 Login 5](#_Toc127951706)

[3.2.2 Certificate/Info 6](#_Toc127951707)

[3.2.3 SignHash 9](#_Toc127951708)

[4 ĐẶC TẢ GIAO TIẾP KÝ BẤT ĐỒNG BỘ 13](#_Toc127951709)

[4.1 Các loại giao dịch 13](#_Toc127951710)

[4.2 Đặc tả chi tiết các giao dịch 13](#_Toc127951711)

[4.2.1 Login 13](#_Toc127951712)

[4.2.2 Certificate/Info 14](#_Toc127951713)

[4.2.3 SignHash 17](#_Toc127951714)

[4.2.4 Get signing request status 20](#_Toc127951715)

[4.3 Danh sách mã lỗi chung 21](#_Toc127951716)

# GIỚI THIỆU

## Mục đích tài liệu

* Tài liệu đặc tả định dạng bản tin và giao thức của hệ thống dịch vụ. Tài liệu được dùng làm liệu để hệ thống của Viettel và các nhà cung cấp ứng dụng giao tiếp.

## Thuật ngữ

| **Thuật ngữ** | **Định nghĩa** | **Ghi chú** |
| --- | --- | --- |
| NSD | Người sử dụng | Khách hàng sử dụng dịch vụ |
| CST | Chứng thư số | Chứng thư số của Khách hàng trên hệ thống Mysign |

## Mô tả tài liệu

Nội dung tài liệu bao gồm các phần sau:

* **Phần I - Giới thiệu**: Giúp người đọc hình dung được nội dung, mục đích và bố cục chung của tài liệu.
* **Phần II – Các luồng xử lý giao tiếp**: Các luồng xử lý nghiệp vụ và luồng giao tiếp bản tin.
* **Phần III – Đặc tả giao tiếp**: Đặc tả giao tiếp chi tiết.

# CÁC LUỒNG XỬ LÝ GIAO TIẾP

## Nghiệp vụ ký điện tử



**Step 1:** Người ký truy cập ứng dụng bên thứ 03.

**Step 2:** Người ký sử dụng ứng dụng bên thứ 3 thực hiện gửi yêu cầu ký.

**Step 3:** Ứng dụng bên thứ 3 sử dụng thư viện thực hiện băm nội dung file (Ví dụ: PDF) cần ký gửi.

**Step 4:** Ứng dụng bên thứ 03 gọi API của Cloud CA với dữ liệu đầu vào là Dữ liệu cần ký định dạng băm.

**Step 5:** Cloud CA tiếp nhận dữ liệu ký, tương tác với SAM tạo yêu cầu xác thực gửi tới Authentication Mobile APP của Cloud CA.

**Step 6:** Người ký xác thực trên Authentication Mobile App bằng mật khẩu, mã PIN, sinh trắc học như vân tay, Face ID…

**Step 7:** Cloud CA nhận được kết quả xác thực, gửi tới SAM. SAM xác thực hợp lệ và ký dữ liệu mã băm trả chữ ký cho ứng dựng bên thứ 3.

**Step 8:** Ứng dựng bên thứ 3 **sử dụng thư viện** tích hợp chữ ký vào file ký tạo file đã ký.

# ĐẶC TẢ GIAO TIẾP KÝ ĐỒNG BỘ

## Các loại giao dịch

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên hàm** | **Mô tả** |
| 1 | Login | Ứng dụng ký đăng nhập và lấy phiên (access\_token) |
| 2 | Certificates/Info | Lấy danh sách Chứng thư số và Thông tin chi tiết từng Chứng thư số của người ký |
| 3 | SignHash | Ký mã băm |

## Đặc tả chi tiết các giao dịch

### **Login**

Ứng dụng ký đăng nhập và lấy phiên (access\_token).

#### Request

|  |  |
| --- | --- |
| Link | BASE\_URL/vtss/service/ras/v1/login |
| HTTP Verb | POST |
| Content Type | application/json |
| Accept | application/json |
| Request Body | { "client\_id": “adss…client”, "client\_secret": “fj49kl…….oOpQS”, "profile\_id": “ADSS RAS Profile 001”, "user\_id": “MST\_0100109106-998” } |

| **ParamePrters** | **Presence** | **Value** | **Description** |
| --- | --- | --- | --- |
| client\_id | MANDATORY | *String* | Client ID của Ứng dụng ký  (Tối đa 50 ký tự). |
| user\_id | MANDATORY | *String* | User ID của người ký  (Tối đa 50 ký tự). |
| client\_secret | MANDATORY | *String* | Khóa bảo mật của Ứng dụng ký |
| profile\_id | MANDATORY | *String* | Profile ID của người ký  (Tối đa 50 ký tự) |

#### Response

|  |  |  |
| --- | --- | --- |
| Status Code | Message | Response Body |
| 200 | OK | { "access\_token": "eyJhbGciOiJIUzI1NsInN…Pcxcz2hM", "refresh\_token": "",  "token\_type": "Bearer",  "expires\_in": "3600" } |
| 400 | Bad Request | { "error": "58071", "error\_description": "The request is missing a required parameter, includes an invalid parameter value, includes a parameter more than once, or is otherwise malformed." } |
| 401 | Unauthorised | { "error": "59033", "error\_description": "Failed to process request - user ID or password is invalid" } |

| **Parameters** | **Presence** | **Value** | **Description** |
| --- | --- | --- | --- |
| access\_token | MANDATORY | String | Phiên giao dịch (access token) |
| refresh\_token | CONDITIONAL | String | Token cập nhật lại phiên giao dịch |
| token\_type | MANDATORY | String | Loại access token |
| expires\_in | MANDATORY | String | Hạn của phiên (seconds) |
| error\_code | CONDITIONAL | String | Mã lỗi. |
| error\_description | CONDITIONAL | String | Mô tả lỗi. |

### **Certificate/Info**

Lấy danh sách Chứng thư số của người ký

#### Request

|  |  |
| --- | --- |
| Link | BASE\_URL/vtss/service/certificates/info |
| HTTP Verb | POST |
| Content Type | application/json |
| Accept | application/json |
| Authorization | Bearer  eyJhbGciOiJIUzI1NsInN…Pcxcz2hM |
| Request Body | {  "client\_id": “adss…client”, "client\_secret": “fj49kl…….oOpQS”, "profile\_id": “ADSS RAS Profile 001”,"user\_id": "MST\_0100109106-998",  "certificates": "chain", "certInfo": true, "authInfo": true} |

| **ParamePrters** | **Presence** | **Value** | **Description** |
| --- | --- | --- | --- |
| client\_id | MANDATORY | *String* | Client ID của Ứng dụng ký  (Tối đa 50 ký tự). |
| user\_id | MANDATORY | *String* | User ID của người ký  (Tối đa 50 ký tự). |
| client\_secret | MANDATORY | *String* | Khóa bảo mật của Ứng dụng ký |
| profile\_id | MANDATORY | *String* | Profile ID của người ký  (Tối đa 50 ký tự) |
| certificates | OPTIONAL | *String* | Chỉ định thông tin Chứng thư số trả về: • **None:** Không • **Single:** Chỉ chứng thư số của người ký  • **Chain:** Cả chuỗi chứng thư số (Certiticate chain). Giá trị mặc định: ‘single’ |
| certInfo | MANDATORY | *Boolean* | • **True:** Trả về các thông tin kèm theo Chứng thư số.  • **False:** Không trả các thông tin kèm theo Chứng thư số.  Giá trị mặc định: ‘false’ |
| authInfo | MANDATORY | *Boolean* | • **True:** Trả về các thông tin về cơ chế ủy quyền được hỗ trợ.  • **False:** Không trả c về các thông tin về cơ chế ủy quyền được hỗ trợ.  Giá trị mặc định: ‘false’ |

#### Responce

|  |  |  |
| --- | --- | --- |
| Status Code | Message | Response Body |
| 200 | OK | [  { "description": "Go>Sign mobile based implicit credential authorization", "key”: { “status": "ENABLED", "algo": [ "1.2.840.113549.1.1.1" ], "len": 2048,  "curve": null }, "cert”: { “status": "valid", "certificates": [ "Base64-encoded X.509 end entity certificate", "Base64-encoded X.509 intermediate CA certificate", "Base64-encoded X.509 issuer CA certificate" ], “issuerDN": "Issuer DN printable string", "SerialNumber": "5AAC41CD8FA22B953640", "subjectDN": "Subject DN printable string", "validFrom": "20180709132216+0000", "validTo": "20190709132216+0000" }, "authMode": "implicit",  "multisign": “2147483647”, "lang": null,  "credential\_id": "0100109106-998\_2475106\_20221011075826",  "SCAL": "2"}  ] |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "The request is missing a required parameter, includes an invalid parameter value, includes a parameter more than once, or is otherwise malformed." } |

| **Parameters** | **Presence** | **Value** | **Description** |
| --- | --- | --- | --- |
| description | OPTIONAL | *String* | Mô tả  (Tối đa 255 ký tự). |
| key/status | MANDATORY | *String* | Trạng thái của cặp khóa của Chứng thư số: • **Enabled:** Khóa có thể sử dùng để ký  • **Disabled:** Không không thể dùng để ký. |
| key/algo | MANDATORY | *String* | Danh sách OIDs các thuật toán ký hỗ trợ. Ví dụ:  • 1.2.840.113549.1.1.1=RSA encryption • 1.2.840.10045.4.3.2=ECDSA with SHA256 |
| key/len | MANDATORY | *Number* | Độ dài khóa (bits). |
| key/curve | CONDITIONAL | *String* | Mã OID của ECDSA curve.  Chỉ trả về khi *keyAlgo* thuộc nhóm ECDSA. |
| cert/status | OPTIONAL | *String* | Trạng thái của Chứng thư số. |
| cert/certificates | CONDITIONAL | *String* | Danh chứng thư số định dạng Base64. |
| cert/issuerDN | CONDITIONAL | *String* | DN của CA cấp CTS  Trả về khi *certInfo* là **“true”**. |
| cert/serialNumber | CONDITIONAL | *String* | Serial number của CTS  Trả về khi *certInfo* là **“true”**. |
| cert/subjectDN | CONDITIONAL | *String* | DN của CTS  Trả về khi *certInfo* là **“true”**. |
| cert/validFrom | CONDITIONAL | *String* | Thời hạn bắt đầu hợp lệ của CTS  Trả về khi *certInfo* là **“true”**.  Định dạng GeneralizedTime (RFC 5280 e.g. “YYYYMMDDHHMMSSZ”). |
| cert/validTo | CONDITIONAL | *String* | Thời hạn kết thúc hợp lệ của CTS  Trả về khi *certInfo* là **“true”**.  Định dạng GeneralizedTime (RFC 5280 e.g. “YYYYMMDDHHMMSSZ”). |
| authMode | MANDATORY | *String* | Phương thức xác thực: • **Implicit:** Việc xác thực do người ký thực hiện. |
| SCAL | OPTIONAL | *String* | • **“2”:** SCAL2 thì mã băm sẽ được liên kết với SAD |
| multisign | MANDATORY | *Number* | Một số bằng hoặc cao hơn 1 đại diện cho số lượng chữ ký tối đa có thể được tạo bằng thông tin xác thực này với một yêu cầu ủy quyền duy nhất. |
| credential\_id | MANDATORY | *String* | Mã credential\_id (định danh) của CTS |
| lang | OPTIONAL | *String* | Mã ngôn ngữ của kết quả theo RFC 5646. |
| error\_code | CONDITIONAL | *String* | Mã lỗi. |
| error\_description | CONDITIONAL | *String* | Mô tả lỗi. |
|  |  |  |  |

### **SignHash**

Xác thực yêu cầu ký.

#### Request

|  |  |
| --- | --- |
| Link | BASE\_URL/vtss/service/signHash |
| HTTP Verb | POST |
| Content Type | application/json |
| Accept | application/json |
| Authorization | Bearer \_TiHRG-bA H3XlFQZ3ndFhkXf9P24/CKN69L8gdSYp5\_pw |
| Request Body | { "credentialID": "JohnDoe",  "client\_id": "samples\_test\_client",  "client\_secret": "12345789qadewaerawer", "numSignatures": 2,  "description": “Document Name”, "documents": [{ "document\_id": 123, "document\_name": “Document Name 123”, },{ "document\_id": 456, "document\_name": “Document Name 456”, }], "hash": [ "sTOgwOm+474gFj0q0x1iSNspKqbcse4IeiqlDg/HWuI=", "c1RPZ3dPbSs0NzRnRmowcTB4MWlTTnNwS3FiY3NlNEllaXFsRGcvSFd1ST0=" ],  "hashAlgo": "2.16.840.1.101.3.4.2.1", "signAlgo": "1.2.840.113549.1.1.1",  “async”: 0 } |

**Request Parameters**

| **Parameters** | **Presence** | **Value** | **Description** |
| --- | --- | --- | --- |
| credentialID | MANDATORY | *String* | ID của Chứng thư số của người ký |
| client\_id | MANDATORY | *String* | Mã client\_id được cung cấp bởi dịch vụ |
| client\_secret | MANDATORY | *String* | Mã client\_secret được cung cấp bởi dịch vụ |
| numSignatures | MANDATORY | *Number* | Số lượng chữ ký cần ký |
| documents/document \_id | MANDATORY | *String* | ID đại diện cho tài liệu ký |
| documents/document \_name | MANDATORY | *String* | \* Tên của tài liệu ký, hiển thị trên yêu cầu ký app Mysign nếu không có thông tin description  \* Để hiển thị chính xác nội dung này, cần truyền thông tin như sau:  - Mã hóa nội dung dạng mã Base64, encode UTF-8 khi truyền vào API  - Độ dài mã Base64 nhỏ hơn 100 kí tự  - Nội dung gốc chỉ được bao hàm các nội dung sau:  + Chữ cái hoa, thường không dấu: a-z, A-Z  + Chữ số: 0-9  + Ký tự đặc biệt: dấu gạch dưới (\_), dấu gạch ngang (-), dấu cách ( ) |
| hash | CONDITIONAL | *String* | Mã băm cải tài liệu ký dạng Base64.  Chỉ tiếp nhận mã hash dạng SHA256 đã chuyển đổi về dạng base64 |
| description | OPTIONAL | *String* | \* Mô tả yêu cầu ký.  \* Nội dung sẽ hiển thị trên yêu cầu ký app Mysign nếu được truyền vào  \* Để hiển thị chính xác nội dung này, cần truyền thông tin như sau:  - Mã hóa nội dung dạng mã Base64, encode UTF-8 khi truyền vào API  - Độ dài mã Base64 nhỏ hơn 100 kí tự  - Nội dung gốc chỉ được bao hàm các nội dung sau:  + Chữ cái hoa, thường không dấu: a-z, A-Z  + Chữ số: 0-9  + Ký tự đặc biệt: dấu gạch dưới (\_), dấu gạch ngang (-), dấu cách ( ) |
| hashAlgo | CONDITIONAL | *String* | Mã OID của thuật toán băm.  Tham số này sẽ bị bỏ qua hoặc bỏ qua nếu thuật toán băm được chỉ định ngầm bởi thuật toán signAlgo. |
| signAlgo | MANDATORY | *String* | OID của thuật toán được sử dụng để ký. Nó sẽ là một trong những giá trị được thông tin xác thực cho phép như được trả về trong *keyAlgo* trong kết quả khi gọi API credentials/info. |
| async | MANDATORY | *Integer* | Chế độ ký đồng bộ/bất đồng bộ  0: Chế độ ký đồng bộ (API sẽ chờ kết quả xác thực từ server)  1: Chế độ ký bất đồng bộ (API sẽ trả mã yêu cầu ký để người dùng gọi hàm kiểm tra)  Ở loại yêu cầu ký này, mã = 0 |

#### Response

|  |  |  |
| --- | --- | --- |
| Status Code | Message | Response Body |
| 200 | OK | { "signatures": [ "KeTob5gl26S2tmXjqN…MRGtoew==" ] } |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "The request is missing a required parameter, includes an invalid parameter value, includes a parameter more than once, or is otherwise malformed." } |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "Missing (or invalid type) string parameter credentialID" } |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "Invalid parameter credentialID" } |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "Missing (or invalid type) integer parameter numSignatures" } |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "Invalid parameter numSignatures" } |

**Response Parameters**

| **Parameters** | **Presence** | **Value** | **Description** |
| --- | --- | --- | --- |
| signatures | MANDATORY | *String* | Danh sách chữ ký dạng base64 tương ứng với danh sách mã băm đầu vào. |
| error\_code | CONDITIONAL | *String* | Mã lỗi. |
| error\_descripti on | CONDITIONAL | *String* | Mô tả lỗi. |

# ĐẶC TẢ GIAO TIẾP KÝ BẤT ĐỒNG BỘ

## Các loại giao dịch

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên hàm** | **Mô tả** |
| 1 | Login | Ứng dụng ký đăng nhập và lấy phiên (access\_token) |
| 2 | Certificates/Info | Lấy danh sách Chứng thư số và Thông tin chi tiết từng Chứng thư số của người ký |
| 3 | SignHash | Ký mã băm (bất đồng bộ) |
| 4 | Get signing request status | Lấy kết quả yêu cầu ký |

## Đặc tả chi tiết các giao dịch

### **Login**

Ứng dụng ký đăng nhập và lấy phiên (access\_token).

#### Request

|  |  |
| --- | --- |
| Link | BASE\_URL/vtss/service/ras/v1/login |
| HTTP Verb | POST |
| Content Type | application/json |
| Accept | application/json |
| Request Body | { "client\_id": “adss…client”, "client\_secret": “fj49kl…….oOpQS”, "profile\_id": “ADSS RAS Profile 001”, "user\_id": “MST\_0100109106-998” } |

| **ParamePrters** | **Presence** | **Value** | **Description** |
| --- | --- | --- | --- |
| client\_id | MANDATORY | *String* | Client ID của Ứng dụng ký  (Tối đa 50 ký tự). |
| user\_id | MANDATORY | *String* | User ID của người ký  (Tối đa 50 ký tự). |
| client\_secret | MANDATORY | *String* | Khóa bảo mật của Ứng dụng ký |
| profile\_id | MANDATORY | *String* | Profile ID của người ký  (Tối đa 50 ký tự) |

#### Response

|  |  |  |
| --- | --- | --- |
| Status Code | Message | Response Body |
| 200 | OK | { "access\_token": "eyJhbGciOiJIUzI1NsInN…Pcxcz2hM", "refresh\_token": "",  "token\_type": "Bearer",  "expires\_in": "3600" } |
| 400 | Bad Request | { "error": "58071", "error\_description": "The request is missing a required parameter, includes an invalid parameter value, includes a parameter more than once, or is otherwise malformed." } |
| 401 | Unauthorised | { "error": "59033", "error\_description": "Failed to process request - user ID or password is invalid" } |

| **Parameters** | **Presence** | **Value** | **Description** |
| --- | --- | --- | --- |
| access\_token | MANDATORY | String | Phiên giao dịch (access token) |
| refresh\_token | CONDITIONAL | String | Token cập nhật lại phiên giao dịch |
| token\_type | MANDATORY | String | Loại access token |
| expires\_in | MANDATORY | String | Hạn của phiên (seconds) |
| error\_code | CONDITIONAL | String | Mã lỗi. |
| error\_description | CONDITIONAL | String | Mô tả lỗi. |

### **Certificate/Info**

Lấy danh sách Chứng thư số của người ký

#### Request

|  |  |
| --- | --- |
| Link | BASE\_URL/vtss/service/certificates/info |
| HTTP Verb | POST |
| Content Type | application/json |
| Accept | application/json |
| Authorization | Bearer  eyJhbGciOiJIUzI1NsInN…Pcxcz2hM |
| Request Body | {  "client\_id": “adss…client”, "client\_secret": “fj49kl…….oOpQS”, "profile\_id": “ADSS RAS Profile 001”,"user\_id": "MST\_0100109106-998",  "certificates": "chain", "certInfo": true, "authInfo": true} |

| **ParamePrters** | **Presence** | **Value** | **Description** |
| --- | --- | --- | --- |
| client\_id | MANDATORY | *String* | Client ID của Ứng dụng ký  (Tối đa 50 ký tự). |
| user\_id | MANDATORY | *String* | User ID của người ký  (Tối đa 50 ký tự). |
| client\_secret | MANDATORY | *String* | Khóa bảo mật của Ứng dụng ký |
| profile\_id | MANDATORY | *String* | Profile ID của người ký  (Tối đa 50 ký tự) |
| certificates | MANDATORY | *String* | Chỉ định thông tin Chứng thư số trả về: • **None:** Không • **Single:** Chỉ chứng thư số của người ký  • **Chain:** Cả chuỗi chứng thư số (Certiticate chain). Giá trị mặc định: ‘single’ |
| certInfo | MANDATORY | *Boolean* | • **True:** Trả về các thông tin kèm theo Chứng thư số.  • **False:** Không trả các thông tin kèm theo Chứng thư số.  Giá trị mặc định: ‘false’ |
| authInfo | MANDATORY | *Boolean* | • **True:** Trả về các thông tin về cơ chế ủy quyền được hỗ trợ.  • **False:** Không trả c về các thông tin về cơ chế ủy quyền được hỗ trợ.  Giá trị mặc định: ‘false’ |

#### Responce

|  |  |  |
| --- | --- | --- |
| Status Code | Message | Response Body |
| 200 | OK | [  { "description": "Go>Sign mobile based implicit credential authorization", "key”: { “status": "ENABLED", "algo": [ "1.2.840.113549.1.1.1" ], "len": 2048,  "curve": null }, "cert”: { “status": "valid", "certificates": [ "Base64-encoded X.509 end entity certificate", "Base64-encoded X.509 intermediate CA certificate", "Base64-encoded X.509 issuer CA certificate" ], “issuerDN": "Issuer DN printable string", "SerialNumber": "5AAC41CD8FA22B953640", "subjectDN": "Subject DN printable string", "validFrom": "20180709132216+0000", "validTo": "20190709132216+0000" }, "authMode": "implicit",  "multisign": “2147483647”, "lang": null,  "credential\_id": "0100109106-998\_2475106\_20221011075826",  "SCAL": "2"}  ] |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "The request is missing a required parameter, includes an invalid parameter value, includes a parameter more than once, or is otherwise malformed." } |

| **Parameters** | **Presence** | **Value** | **Description** |
| --- | --- | --- | --- |
| description | OPTIONAL | *String* | Mô tả  (Tối đa 255 ký tự). |
| key/status | MANDATORY | *String* | Trạng thái của cặp khóa của Chứng thư số: • **Enabled:** Khóa có thể sử dùng để ký  • **Disabled:** Không không thể dùng để ký. |
| key/algo | MANDATORY | *String* | Danh sách OIDs các thuật toán ký hỗ trợ. Ví dụ:  • 1.2.840.113549.1.1.1=RSA encryption • 1.2.840.10045.4.3.2=ECDSA with SHA256 |
| key/len | MANDATORY | *Number* | Độ dài khóa (bits). |
| key/curve | CONDITIONAL | *String* | Mã OID của ECDSA curve.  Chỉ trả về khi *keyAlgo* thuộc nhóm ECDSA. |
| cert/status | OPTIONAL | *String* | Trạng thái của Chứng thư số. |
| cert/certificates | CONDITIONAL | *String* | Danh chứng thư số định dạng Base64. |
| cert/issuerDN | CONDITIONAL | *String* | DN của CA cấp CTS  Trả về khi *certInfo* là **“true”**. |
| cert/serialNumber | CONDITIONAL | *String* | Serial number của CTS  Trả về khi *certInfo* là **“true”**. |
| cert/subjectDN | CONDITIONAL | *String* | DN của CTS  Trả về khi *certInfo* là **“true”**. |
| cert/validFrom | CONDITIONAL | *String* | Thời hạn bắt đầu hợp lệ của CTS  Trả về khi *certInfo* là **“true”**.  Định dạng GeneralizedTime (RFC 5280 e.g. “YYYYMMDDHHMMSSZ”). |
| cert/validTo | CONDITIONAL | *String* | Thời hạn kết thúc hợp lệ của CTS  Trả về khi *certInfo* là **“true”**.  Định dạng GeneralizedTime (RFC 5280 e.g. “YYYYMMDDHHMMSSZ”). |
| authMode | MANDATORY | *String* | Phương thức xác thực: • **Implicit:** Việc xác thực do người ký thực hiện. |
| SCAL | OPTIONAL | *String* | • **“2”:** SCAL2 thì mã băm sẽ được liên kết với SAD |
| multisign | MANDATORY | *Number* | Một số bằng hoặc cao hơn 1 đại diện cho số lượng chữ ký tối đa có thể được tạo bằng thông tin xác thực này với một yêu cầu ủy quyền duy nhất. |
| credential\_id | MANDATORY | *String* | Mã credential\_id (định danh) của CTS |
| lang | OPTIONAL | *String* | Mã ngôn ngữ của kết quả theo RFC 5646. |
| error\_code | CONDITIONAL | *String* | Mã lỗi. |
| error\_description | CONDITIONAL | *String* | Mô tả lỗi. |
|  |  |  |  |

### **SignHash**

Xác thực yêu cầu ký.

#### Request

|  |  |
| --- | --- |
| Link | BASE\_URL/vtss/service/signHash |
| HTTP Verb | POST |
| Content Type | application/json |
| Accept | application/json |
| Authorization | Bearer \_TiHRG-bA H3XlFQZ3ndFhkXf9P24/CKN69L8gdSYp5\_pw |
| Request Body | { "credentialID": "JohnDoe",  "client\_id": "samples\_test\_client",  "client\_secret": "12345789qadewaerawer", "numSignatures": 2,  "description": “Document Name”, "documents": [{ "document\_id": 123, "document\_name": “Document Name 123”, },{ "document\_id": 456, "document\_name": “Document Name 456”, }], "hash": [ "sTOgwOm+474gFj0q0x1iSNspKqbcse4IeiqlDg/HWuI=", "c1RPZ3dPbSs0NzRnRmowcTB4MWlTTnNwS3FiY3NlNEllaXFsRGcvSFd1ST0=" ],  "hashAlgo": "2.16.840.1.101.3.4.2.1", "signAlgo": "1.2.840.113549.1.1.1",  “async”: 1 } |

**Request Parameters**

| **Parameters** | **Presence** | **Value** | **Description** |
| --- | --- | --- | --- |
| credentialID | MANDATORY | *String* | ID của Chứng thư số của người ký |
| client\_id | MANDATORY | *String* | Mã client\_id được cung cấp bởi dịch vụ |
| client\_secret | MANDATORY | *String* | Mã client\_secret được cung cấp bởi dịch vụ |
| numSignatures | MANDATORY | *Number* | Số lượng chữ ký cần ký |
| documents/document \_id | MANDATORY | *String* | ID đại diện cho tài liệu ký |
| documents/document \_name | MANDATORY | *String* | \* Tên của tài liệu ký, hiển thị trên yêu cầu ký app Mysign nếu không có thông tin description  \* Để hiển thị chính xác nội dung này, cần truyền thông tin như sau:  - Mã hóa nội dung dạng mã Base64, encode UTF-8 khi truyền vào API  - Độ dài mã Base64 nhỏ hơn 100 kí tự  - Nội dung gốc chỉ được bao hàm các nội dung sau:  + Chữ cái hoa, thường không dấu: a-z, A-Z  + Chữ số: 0-9  + Ký tự đặc biệt: dấu gạch dưới (\_), dấu gạch ngang (-), dấu cách ( ) |
| hash | MANDATORY | *String* | Mã băm cải tài liệu ký dạng Base64 |
| description | MANDATORY | *String* | \* Mô tả yêu cầu ký.  \* Nội dung sẽ hiển thị trên yêu cầu ký app Mysign nếu được truyền vào  \* Để hiển thị chính xác nội dung này, cần truyền thông tin như sau:  - Mã hóa nội dung dạng mã Base64, encode UTF-8 khi truyền vào API  - Độ dài mã Base64 nhỏ hơn 100 kí tự  - Nội dung gốc chỉ được bao hàm các nội dung sau:  + Chữ cái hoa, thường không dấu: a-z, A-Z  + Chữ số: 0-9  + Ký tự đặc biệt: dấu gạch dưới (\_), dấu gạch ngang (-), dấu cách ( ) |
| hashAlgo | CONDITIONAL | *String* | Mã OID của thuật toán băm.  Tham số này sẽ bị bỏ qua hoặc bỏ qua nếu thuật toán băm được chỉ định ngầm bởi thuật toán signAlgo. |
| signAlgo | MANDATORY | *String* | OID của thuật toán được sử dụng để ký. Nó sẽ là một trong những giá trị được thông tin xác thực cho phép như được trả về trong *keyAlgo* trong kết quả khi gọi API credentials/info. |
| async | MANDATORY | *Integer* | Chế độ ký đồng bộ/bất đồng bộ  0: Chế độ ký đồng bộ (API sẽ chờ kết quả xác thực từ server)  1: Chế độ ký bất đồng bộ (API sẽ trả mã yêu cầu ký để người dùng gọi hàm kiểm tra)  Ở loại yêu cầu ký này, mã = 0 |

#### Response

|  |  |  |
| --- | --- | --- |
| Status Code | Message | Response Body |
| 200 | OK | { "transactionId": "de67f948-0498-4919-af28-dff54a6a4e77" } |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "The request is missing a required parameter, includes an invalid parameter value, includes a parameter more than once, or is otherwise malformed." } |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "Missing (or invalid type) string parameter credentialID" } |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "Invalid parameter credentialID" } |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "Missing (or invalid type) integer parameter numSignatures" } |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "Invalid parameter numSignatures" } |

**Response Parameters**

| **Parameters** | **Presence** | **Value** | **Description** |
| --- | --- | --- | --- |
| signatures | MANDATORY | *String* | Danh sách chữ ký dạng base64 tương ứng với danh sách mã băm đầu vào. |
| error\_code | CONDITIONAL | *String* | Mã lỗi. |
| error\_descripti on | CONDITIONAL | *String* | Mô tả lỗi. |

### **Get signing request status**

Xác thực yêu cầu ký.

#### Request

|  |  |
| --- | --- |
| Link | BASE\_URL/vtss/service/requests/status |
| HTTP Verb | POST |
| Content Type | application/json |
| Accept | application/json |
| Authorization | Bearer \_TiHRG-bA H3XlFQZ3ndFhkXf9P24/CKN69L8gdSYp5\_pw |
| Request Body | { “transactionId”: “de67f948-0498-4919-af28-dff54a6a4e77”  } |

**Request Parameters**

| **Parameters** | **Presence** | **Value** | **Description** |
| --- | --- | --- | --- |
| transactionId | MANDATORY | *String* | ID của Yêu cầu ký cần tra kết quả |

#### Response

|  |  |  |
| --- | --- | --- |
| Status Code | Message | Response Body |
| 200 | OK | { "signatures": [ "KeTob5gl26S2tmXjqN…MRGtoew==" ],  "status": "1" } |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "The request is missing a required parameter, includes an invalid parameter value, includes a parameter more than once, or is otherwise malformed." } |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "Missing (or invalid type) string parameter credentialID" } |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "Invalid parameter credentialID" } |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "Missing (or invalid type) integer parameter numSignatures" } |
| 400 | Bad Request | { "error": "invalid\_request", "error\_description": "Invalid parameter numSignatures" } |

**Response Parameters**

| **Parameters** | **Presence** | **Value** | **Description** |
| --- | --- | --- | --- |
| signatures | MANDATORY | *String* | Danh sách chữ ký dạng base64 tương ứng với danh sách mã băm đầu vào. |
| status | MANDATORY | *String* | Mã trạng thái của yêu cầu ký đang tra cứu:  1 – Success  4000 – Chờ người dùng xác nhận  4001 – Yêu cầu ký hết thời gian chờ (Timeout)  4002 – Người dùng từ chối ký  4004 – Ký thất bại (có lỗi xảy ra)  50000 – Có lỗi xảy ra khi lấy thông tin |
| error\_code | CONDITIONAL | *String* | Mã lỗi. |
| error\_descripti on | CONDITIONAL | *String* | Mô tả lỗi. |

## Danh sách mã lỗi chung

| **Mã lỗi** | **Mô tả lỗi** |
| --- | --- |
| 58001 | An internal server error occurred while processing the request – see the RAS service debug logs for details |
| 58002 | Service is not available - Try later |
| 58003 | Failed to process request - RAS service is not enabled in license |
| 58004 | Failed to process request - RAS service license has expired |
| 58005 | Failed to process request - RAS service is not enabled in system |
| 58006 | Failed to process request - RAS service is not allowed |
| 58007 | Failed to process request - Client ID does not exist |
| 58008 | Failed to process request - User ID does not exist |
| 58009 | Failed to process request - User ID already exists |
| 58010 | Failed to process request - Key alias does not exist |
| 58011 | Failed to process request - Transaction ID does not exist |
| 58012 | Failed to process request - Client ID not found in the request |
| 58013 | Failed to process request - User ID not found in the request |
| 58014 | Failed to process request - Key alias not found in the request |
| 58015 | Failed to process request - Subject DN not found in the request |
| 58016 | Failed to process request - User password not found in the request |
| 58017 | Failed to process request - Key length not found in the request |
| 58018 | Failed to process request - Key algorithm not found in the request |
| 58019 | Failed to process request - User name not found in the request |
| 58020 | Failed to process request - User password not found in the request |
| 58021 | Failed to process request - User mobile number not found in the request |
| 58022 | Failed to process request - Key alias exceeds the allowed limit |
| 58023 | Failed to process request - User ID exceeds the allowed limit |
| 58024 | Failed to process request - User name exceeds the allowed limit |
| 58025 | Failed to process request - User password exceeds the allowed limit |
| 58026 | Failed to process request - Invalid user mobile number |
| 58027 | Failed to process request - Invalid user email |
| 58028 | Failed to process request - Invalid user status |
| 58029 | Failed to process request - RAS profile does not exist or marked inactive |
| 58030 | Failed to process request - User certificate not found in the request |
| 58031 | Failed to process request - Profile ID not found in the request |
| 58032 | Failed to process request - Invalid client ID |
| 58033 | Failed to process request - User's new password not found in the request |
| 58034 | Failed to process request - SMS OTP not found in the request |
| 58035 | Failed to process request - Email OTP not found in the request |
| 58036 | Invalid string parameter - refresh\_token |
| 58037 | Failed to process request - Invalid refresh token |
| 58038 | Failed to process request - Invalid access token |
| 58039 | The request is missing a required parameter, includes an invalid parameter value, includes a parameter more than once, or is otherwise malformed. |
| 58040 | Failed to process request - Basic authentication is not enabled in RAS profile |
| 58041 | Failed to process request - SAML authentication is not enabled in RAS profile |
| 58042 | Failed to process request - Missing (or invalid type) string parameter token |
| 58043 | Failed to process request - Invalid string parameter token\_type\_hint |
| 58044 | Failed to process request - Invalid string parameter token |
| 58045 | Failed to process request - Client ID is not configured for certification service settings in RAS service manager |
| 58046 | Failed to process request - Certification profile is not configured for certification service settings in RAS service manager |
| 58047 | Failed to process request - Certification service address is not configured for certification service settings in RAS service manager |
| 58048 | Failed to process request - Unable to get device certificate from certification service |
| 58049 | Failed to generate access token - HMAC Key not configured in RAS service manager |
| 58050 | Failed to process request - User Email not found in the request |
| 58051 | Failed to process request - Client ID is not configured for default settings in RAS service manager |
| 58052 | Failed to process request - Device ID not found in the request |
| 58053 | Failed to process request - Push notification token not found in the request |
| 58054 | Failed to process request - OS type not found in the request |
| 58055 | Missing (or invalid type) string parameter credentialID |
| 58056 | Missing (or invalid type) integer parameter numSignatures |
| 58057 | Invalid parameter numSignatures |
| 58058 | Invalid request parameter - numSignatures doesn't match with no of hashes in hash array |
| 58059 | Invalid request parameter - no of documents in clientData doesn't match with no of hashes in hash array |
| 58060 | Missing parameter hash |
| 58061 | Failed to authorise user credentials - Request timeout for mobile authorisation |
| 58062 | Failed to authorise user credentials - User cancelled mobile authorisation |
| 58063 | Invalid parameter credentialID |
| 58064 | Missing (or invalid type) string parameter SAD |
| 58065 | Invalid parameter SAD |
| 58066 | Empty hash array |
| 58067 | Invalid Base64 hash string parameter |
| 58068 | Missing (or invalid type) string parameter signAlgo |
| 58069 | Invalid parameter signAlgo |
| 58070 | Missing (or invalid type) string parameter hashAlgo |
| 58071 | Invalid parameter hashAlgo |
| 58072 | Failed to validate SAML assertion - Invalid base64 data |
| 58073 | Failed to validate SAML assertion - Not comply with SAML 2.0 schema |
| 58074 | Failed to validate SAML assertion - Unable to parse SAML assertion |
| 58075 | Failed to validate SAML assertion - Validity period expired or not yet valid |
| 58076 | Failed to validate SAML assertion - Server certificate does not match with the certificate configured in RAS Profile |
| 58077 | Failed to validate SAML assertion - Multiple or no attributeValue found |
| 58078 | Failed to validate SAML assertion - Invalid Signature |
| 58079 | Failed to process request - User status is blocked or inactive |
| 58080 | Failed to process request - Certificate chain not found in the request |
| 58081 | Failed to process request - Invalid certificate chain |
| 58082 | Failed to process request - Client secret not found in the request |
| 58083 | Failed to authorise user credentials - An internal server error occurred during signature computation |
| 58084 | Failed to process request - Device CSR not found in the request |
| 58085 | Failed to process request - Invalid device CSR |
| 58086 | Failed to process request - Device information not found in the request |
| 58087 | Failed to process request - Device ID not found in the request |
| 58088 | Failed to process request - Device name not found in the request |
| 58089 | Failed to process request - SAD not found in the request |
| 58090 | Failed to process request - Request ID not found in the request |
| 58091 | Failed to process request - Invalid request |
| 58092 | Failed to process request - Either request ID is invalid or the transaction is expired |
| 58093 | An internal server error occurred - please contact your service provider |
| 58094 | Failed to process request - User mobile exceeds the allowed limit |
| 58095 | Failed to process request - User email exceeds the allowed limit |
| 58096 | Failed to process request - Configurations for SMS/Email OTP(s) not available |
| 58097 | Failed to process request - No OTP(s) found in request |
| 58098 | Failed to process request - QR Code authentication is not allowed for this RAS profile |
| 86000 | Failed to authenticate client - TLS client authentication certificate has expired |
| 86001 | Failed to authenticate client - TLS certificate CN does not match with Client ID |
| 86002 | Failed to authenticate client - TLS client certificate is revoked |
| 86003 | Failed to authenticate client - revocation status for TLS client certificate is unknown |
| 86004 | Failed to authenticate client - Client ID does not match with the client identified by TLS client certificate |
| 86005 | Failed to authenticate client - TLS client certificate does not match with the configured client certificate |
| 86006 | Failed to authenticate client - request signing certificate has expired |
| 86007 | Failed to authenticate client - request signing certificate is revoked |
| 86008 | Failed to authenticate client - revocation status for request signing certificate is unknown |
| 86009 | Failed to authenticate client - request signing certificate does not match with the configured client certificate |
| 86010 | Failed to authenticate client - Client ID does not match with the client identified by the request signing certificate |
| 86011 | Failed to authenticate client - Client ID does not exist |
| 86012 | An error occurred while communicating with database - see the service debug logs for details |
| 86013 | An error occurred when checking the certificate revocation status see the service debug logs for details |
| 86014 | An internal error occurred while authenticating the client - see the service debug logs for details |
| 86015 | Failed to authenticate client - Client ID is not found in the request |
| 86016 | Failed to process request - Request signing certificate is not trusted |
| 86017 | Failed to authenticate client - client is marked inactive |
| 86018 | Failed to authorise client - service is not allowed to this client |
| 86019 | Failed to authorise client - service profile does not exist |
| 86020 | Failed to authorise client - service profile is inactive |
| 86021 | Failed to authorise client - profile is not allowed to this client |
| 86022 | Failed to authorise client - default profile not configured and neither found in request |
| 86023 | Failed to authorise client - default profile is inactive |
| 86024 | Failed to authorise client - client secret is invalid |
| internal\_error | An internal server error occurred while processing the request |
| invalid\_csr | CSR is invalid |
| invalid\_otp | OTP is either invalid or expired |
| missing\_csr | CSR is missing in the request |
| missing\_device\_id | Device ID is missing in the request |
| missing\_device\_info | Device information is missing in the request |
| missing\_device\_name | Device name is missing in the request |
| missing\_request\_id | Request ID is missing in the request |
| refresh\_token\_revoke d | Refresh token is either invalid or expired |