TÍCH HỢP HỆ THỐNG LƯU TRỮ CHỨNG THƯ VÀ KÝ SỐ ONLINE - CYBERSIGN

Phiên bản: 1.3

MỤC LỤC

1. Một số mô hình triển khai 4
1.1. Ký số file 4
1.2. Ký sồ hash file 4
2. Mô tả các đầu hàm kết nối 5
2.1. Authorization (Xác thực) 5
2.1.1. Cấu trúc xác thực 6
2.1.2. Tạo chữ ký HMAC (signature digest) 6
2.2. Lấy thông tin tài khoản 7
2.3. Lấy thông tin chứng thư số 8
2.4. Lấy thông tin chứng thư số sub 9
2.5. Lấy thông tin chứng thư số root 10
2.6. Lấy chain của chứng thư số 11
2.7. Lấy thông tin dịch vụ 11
2.8. Lấy lịch sử giao dịch 12
2.9. Xác thực chứng thư số 14
2.10. Ký file tài liệu dạng PDF 15
2.11. Ký hash file PDF 17
2.12. Ký file định dạng Office 18
2.13. Ký hash file Office 19
2.14. Ký file định dạng XML 21
2.15. Xác thực file Office 22

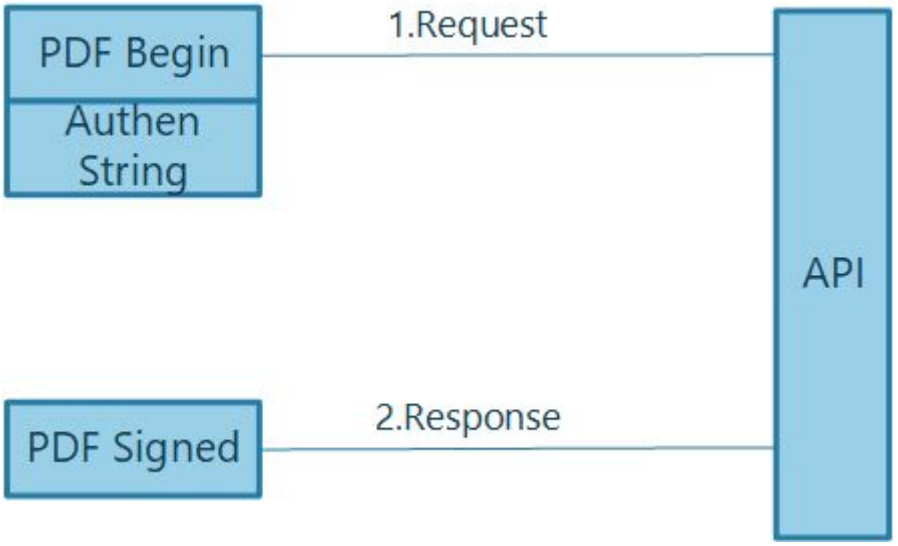
Các phiên bản

Phiên bản	Ngày phát hành	Các sửa đổi	Ghi chú
1.0	02-11-2018		Hướng dẫn sơ bộ
1.3	08-11-2018	Thêm mô hình triển khai	Bổ sung mô hình để rõ hơn cho người lập trình kết nối

1. Một số mô hình triển khai

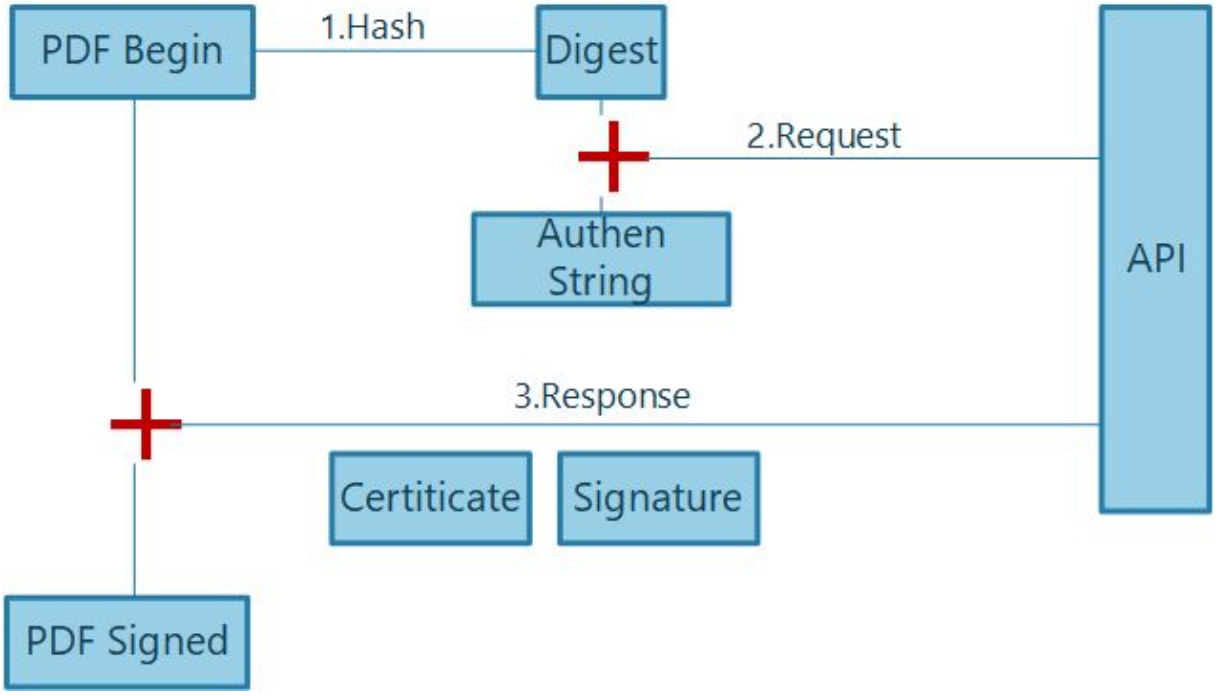
1.1. Ký số file

Ký cả file:



1.2. Ký số hash file

Ký dữ liệu băm:



Bước 1: Phần mềm phía đối tác thực hiện băm (Hash) file PDF thành dạng byte (Digest)
Bước 2: Sử dụng phương thức kết nối đã thống nhất, gửi dữ liệu dạng băm lên hệ thống CyberLotus
Bước 3: Hệ thống của CyberLotus thực hiện kiểm tra người dùng và ký số, trả về chữ ký tương ứng với dữ liệu băm
Bước 4: Phần mềm phía đối tác thực hiện ghép chữ ký số vào file, và lưu trữ lại file PDF đã ký

2. Mô tả các đầu hàm kết nối

2.1. Authorization (Xác thực)

Đối với các yêu cầu gửi lên hệ thống, cần được xác thực trước khi thực hiện. Để an toàn và tránh DDOS, hệ thống CyberSign ứng dụng chuẩn HMAC vào xác thực.
Ví dụ về cấu trúc service gửi dữ liệu băn ký số file office. Cấu trúc service này được mô tả trong hệ thống như sau:

```
POST /api/office/sign/hashdata HTTP/1.1
Host: api.hsm.cyberlotus.com:8080
Content-Type: application/json; charset=utf-8
Date: "Wed, 22 May 2019 11:05:51 GMT"
Authorization: HmacSHA256
CyberLotus123:515919404b16472485ec496a32d58178:3JiCBWv84CCj6dtg28TY2Kpmb1fw
TfsiGuC4jiFuEho=:1558523152
{\"base64digest\":\"SGFja2VyUmFuaw==\",\"hashalg\":\"SHA-1\"}
```

Trong đó mô tả các thuật ngữ:

POST	HttpMethod Phướng thức của HTTP bao gồm: POST, GET, PUT, DELETE
HTTP/1.1	Giao thức kết nối
api.hsm.cyberlotus.com:8080	Host và Port kết nối
/api/office/sign/hashdata	Đường dẫn kết nối
Content-Type	Loại thể hiện: application/json; charset=utf-8
Date	Thời gian gửi yêu cầu
Authorization	Chuỗi xác thực
{ \"base64digest\":\"SGFja2VyUmFuaw==\", \"hashalg\":\"SHA-1\" }	Đây là cấu trúc dữ liệu gửi đi, ví dụ: - Biến: base64digest → Giá trị: SGFja2VyUmFuaw== - Biến: hashalg → Giá trị: SHA-1

Tài liệu sẽ mô tả chi tiết cấu trúc và cách tạo ra chuỗi xác thực

2.1.1. Mô tả cấu trúc

Header tag	Cấu trúc	Ví dụ
Date	Chuỗi DateTime thời điểm gửi request theo định dạng RFC822. Tham khảo https://tools.ietf.org/html/rfc822	"Wed, 22 May 2019 11:05:51 GMT"
Authorization	{hmac_algorithm} {api_id}:{nonce}:{ signature digest}:{timestamp} Trong đó: - **hmac_algorithm**: Thuật toán HmacSHA256 - **api_id**: Mã ứng dụng được cấp theo tài khoản sử dụng dịch vụ - **nonce**: Chuỗi ngẫu nhiên độ dài tối đa 128 bit - **signature digest**: Chữ ký HMAC theo mỗi request theo chuẩn https://tools.ietf.org/html/rfc2104 HMAC-SHA256 với khóa được cấp theo tài khoản sử dụng dịch vụ **timestamp**: Là số giây bắt đầu từ thời điểm 1/1/1970 00:00:00 GMT tới thời điểm hiện tại.(Unix timestamp)	Authorization: HmacSHA256 CyberLotus123:51591940 4b16472485ec496a32d58 178:3JiCBWv84CCj6dtg28 TY2Kpmb1fwTfsiGuC4jiFu Eho=:1558523152

2.1.2. Tạo chữ ký HMAC (signature digest)

Bước 1: Tạo dữ liệu cần ký (SignatureRaw)
Dữ liệu đầu vào được sinh từ request gửi đến server theo từng hàng với thứ tự như sau:

POST *http* *api.hsm.cyberlotus.com:8080* */api/office/sign/hashdata* *application/json; charset=utf-8* *CyberLotus123* *515919404b16472485ec496a32d58178* *Wed, 22 May 2019 11:05:51 GMT* *{\"base64digest\":\"SGFja2VyUmFuaw==\",\"hashalg\":\"SHA-1\"}*	HttpMethod Giao thức {host}:{port} link ContentType API_ID nonce Date Message

- **Hàng 1**: "HttpMethod"
  - Ví dụ: POST GET PUT DELETE
- **Hàng 2**: Giao thức kết nối
  - Ví dụ: http, https
- **Hàng 3**: Host và port kết nối {host}:{port}
  - Ví dụ: api.hsm.cyberlotus.com:8080

- **Hàng 4**: Đường dẫn kết nối
  - Ví dụ: /api/account/info
- **Hàng 5**: ContentType nếu có nội dung gửi đi
  - Ví dụ: “application/json”
- **Hàng 6**: API_ID
  - Ví dụ: *CyberLotus123* (Được cấp bởi nhà cung cấp)
- **Hàng 7**: nonce
  - Chuỗi ngẫu nhiên độ dài tối đa 128 bit
- **Hàng 8**: Date
  - Chuỗi DateTime thời điểm gửi request theo định dạng RFC822.
- **Hàng 9**: Nội dung Message gửi đi

Ghi chú: Kí tự phân dòng ‘\n’ Mã ascii 13

Bước 2: Hàm tạo chữ ký

Signature = Base64ENCODE(HMAC-SHA256(Base64DECODE(**SecretKey**), **SignatureRaw**)));

Ví dụ cụ thể:

- Khóa được nhà cung cấp bàn giao

API_ID	CyberLotus123
SecretKey	Q3liZXJMb3R1c0AxMjM=

- Giá trị chữ ký tính được

SignatureRaw	POST\nhttp\napi.hsm.cyberlotus.com:8080\n/api/office/sign/hashdata\napplication/json; charset=utf-8\nCyberLotus123\n515919404b16472485ec496a32d58178\nWed, 22 May 2019 11:05:51 GMT\n{\"base64digest\":\"SGFja2VyUmFuaw==\",\"hashalg\":\"SHA-1\"}\n
SecretKey	Q3liZXJMb3R1c0AxMjM=
Chữ ký HMAC (***Signature digest)***	3JiCBWv84CCj6dtg28TY2Kpmb1fwTfsiGuC4jiFuEho=

2.2. Lấy thông tin tài khoản

Cấu trúc dữ liệu gửi lên

Trường	**Dữ liệu**

Request Method	GET
Request URL	http://10.0.15.164/api/account/info
Request Header Content-Type	application/json
Authorization	Type: hmac

Cấu trúc dữ liệu trả về

Trường	Dữ liệu
Header status	200 - Success, 401 Unauthorized , 404 - Not Found
Header Content-Type	application/json;charset=UTF-8

Form data	{
	“khachhang_mst”: “String”,
	“khachhang_ten”: “String”,
	“khachhang_diachi”: “String”
	}

Mô tả

TT	Tên biến	Kiểu	Mô tả
1	khachhang_mst	String	Mã số thuế khách hàng
2	khachhang_ten	String	Tên đăng ký sử dụng của khách hàng
3	khachhang_diachi	String	Địa chỉ khách hàng

2.3. Lấy thông tin chứng thư số

Cấu trúc dữ liệu gửi lên

Trường	Dữ liệu
Request Method	GET
Request URL	http://10.0.15.164/api/account/endcert

Request Header Content-Type	application/json
Authorization	Type: hmac

Cấu trúc dữ liệu trả về

Trường	Dữ liệu
Header status	200 - Success, 401 Unauthorized , 404 - Not Found
Header Content-Type	application/json;charset=UTF-8
Form data	String

Mô tả

TT	Kiểu	Mô tả
1	String	Base64 của chứng thư số người dùng cuối

2.4. Lấy thông tin chứng thư số sub

Cấu trúc dữ liệu gửi lên

Trường	Dữ liệu
Request Method	GET
Request URL	http://10.0.15.164/api/account/subcert
Request Header Content-Type	application/json
Authorization	Type: hmac

Cấu trúc dữ liệu trả về

Trường	Dữ liệu
Header status	200 - Success, 401 Unauthorized , 404 - Not Found
Header Content-Type	application/json;charset=UTF-8

Form data	String

Mô tả

TT	Kiểu	Mô tả
1	String	Base64 của chứng thư số người dùng cuối

2.5. Lấy thông tin chứng thư số root

Cấu trúc dữ liệu gửi lên

Trường	Dữ liệu
Request Method	GET
Request URL	http://10.0.15.164/api/account/rootcert
Request Header Content-Type	application/json
Authorization	Type: hmac

Cấu trúc dữ liệu trả về

Trường	Dữ liệu
Header status	200 - Success, 401 Unauthorized , 404 - Not Found
Header Content-Type	application/json;charset=UTF-8
Form data	String

Mô tả

TT	Kiểu	Mô tả
1	String	Base64 của chứng thư số người dùng cuối

2.6. Lấy chain của chứng thư số

Cấu trúc dữ liệu gửi lên

Trường	Dữ liệu
Request Method	GET
Request URL	http://10.0.15.164/api/account/certchain
Request Header Content-Type	application/json
Authorization	Type: hmac

Cấu trúc dữ liệu trả về

Trường	Dữ liệu
Header status	200 - Success, 401 Unauthorized , 404 - Not Found
Header Content-Type	application/json;charset=UTF-8
Form data	String

Mô tả

TT	Kiểu	Mô tả
1	String	Base64 của chứng thư số người dùng cuối

2.7. Lấy thông tin dịch vụ

Cấu trúc dữ liệu gửi lên

Trường	Dữ liệu
Request Method	POST
Request URL	http://10.0.15.164/api/account/service
Request Header Content-Type	application/json
Authorization	Type: hmac

Cấu trúc dữ liệu trả về

Trường	Dữ liệu
Header status	200 - Success, 401 Unauthorized , 404 - Not Found
Header Content-Type	application/json;charset=UTF-8

Form data	{
	“dichvu_ten”: “String”,
	“dichvu_batdau”: “String”,
	“dichvu_ketthuc”: “String”,
	“dichvu_trangthai”: “String”
	}

Mô tả

TT	Tên biến	Kiểu	Mô tả
1	dichvu_ten	String	Tên gói dịch vụ
2	dichvu_batdau	String	Thời điểm bắt đầu gói dịch vụ
3	dichvu_ketthuc	String	Thời điểm kết thúc gói dịch vụ
4	dichvu_trangthai	String	Trạng thái hoạt động của gói dịch vụ

2.8. Lấy lịch sử giao dịch

Cấu trúc dữ liệu gửi lên

Trường	Dữ liệu
Request Method	GET
Request URL	http://10.0.15.164/api/account/service
Request Header Content-Type	application/json
Authorization	Type: hmac
Form data	{

	“batdau”: “String”, “ketthuc”: “String” }

Mô tả

TT	Tên biến	Kiểu	Mô tả
1	batdau	String	Thời gian bắt đầu tra cứu
2	ketthuc	String	Thời gian kết thúc tra cứu

Cấu trúc dữ liệu trả về

Trường	Dữ liệu
Header status	200 - Success, 401 Unauthorized , 404 - Not Found
Header Content-Type	application/json;charset=UTF-8
Form data	List<Auditlogs_out>

Mô tả: **Auditlogs_out**

Auditlogs_out	{
	“thoigian”: “String”,
	“thoigian_tieuton”: “int”,
	“loi_controller”: “String”,
	“loi_function”: “String”,
	“loi_thongtin”: “String”,
	“loi_loai”: “int”
	}

Mô tả

TT	Tên biến	Kiểu	Mô tả

1	thoigian	String	Thời gian gọi lên thực hiện
2	thoigian_tieuton	int	Thời gian xử lý yêu cầu
3	loi_controller	String	Thông tin lỗi nằm trong yêu cầu nào
4	loi_function	String	Hàm thực hiện yêu cầu
5	loi_thongtin	String	Thông tin thực hiện
6	loi_loai	int	Loại lỗi

2.9. Xác thực chứng thư số

Cấu trúc dữ liệu gửi lên

Trường	Dữ liệu
Request Method	GET
Request URL	http://10.0.15.164/api/certificate/verify
Request Header Content-Type	application/json
Authorization	Type: hmac

Form data	{
	“base64Cert”: “String”
	}

Mô tả

TT	Tên biến	Kiểu	Mô tả
1	base64Cert	String	Base64 của chứng thư số

Cấu trúc dữ liệu trả về

Trường	Dữ liệu
Header status	200 - Success, 401 Unauthorized , 404 - Not Found

Header Content-Type	application/json;charset=UTF-8

Form data	{
	“code”: “int”,
	“message”: “String”
	}

Mô tả

TT	Tên biến	Kiểu	Mô tả
1	code	int	Giá trị trả về hàm xác thực chứng thư
2	message	String	Mô tả giá trị trả về

2.10. Ký file tài liệu dạng PDF

Cấu trúc dữ liệu gửi lên

Trường	Dữ liệu
Request Method	POST
Request URL	http://10.0.15.164/api/pdf/sign/originaldata
Request Header Content-Type	application/json
Authorization	Type: hmac
Form data	{ “base64pdf”: “String”, “hashalg”: “String”, “typesignature”: “int”, “signaturename”: “String”, “base64image”: “String”, “textout”: “String”, “pagesign”: “int”, “xpoint”: “int”, “ypoint”: “int”, “width”: “int”,

	“height”: “int” }

Mô tả

TT	Tên biến	Kiểu	Mô tả
1	base64pdf	String	Base64 của file PDF cần ký
2	hashalg	String	Thuật toán hàm băm: SHA1, SHA256, SHA512
3	typesignature	int	Loại hiển thị chữ ký: 0 - Không hiển thị chữ ký 1 - Hiển thị dưới dạng text 2 - Hiển thị dưới dạng hình ảnh 3 - Hiển thị cả hình ảnh và text
4	signaturename	String	Tên của vị trí ký (trường hợp có vị trí)
5	base64image	String	Base64 của hình ảnh (trong trường hợp muốn hiển thị hình ảnh)
6	textout	String	Chuỗi text sẽ hiển thị lên (trong trường hợp muốn hiển thị text)
7	pagesign	int	Trang hiển thị chữ ký, trong trường hợp chọn có hiển thị
8	xpoint	int	Tọa độ X của khung chữ ký
9	ypoint	int	Tọa độ Y của khung chữ ký
10	width	int	Độ rộng của khung chữ ký
11	height	int	Độ cao của khung chữ ký

Cấu trúc dữ liệu trả về

Trường	Dữ liệu
Header status	200 - Success, 401 Unauthorized , 404 - Not Found

Header Content-Type	application/json;charset=UTF-8

Form data	{
	“base64pdfSigned”: “String”,
	“status”: “int”,
	“description”: “String”
	}

Mô tả

TT	Tên biến	Kiểu	Mô tả
1	base64pdfSigned	String	Base64 của file PDF đã có chữ ký
2	status	int	Mã lỗi của hàm ký số
3	description	String	Mô tả lỗi của hàm ký số

2.11. Ký hash file PDF

Cấu trúc dữ liệu gửi lên

Trường	Dữ liệu
Request Method	POST
Request URL	http://10.0.15.164/api/pdf/sign/hashdata
Request Header Content-Type	application/json
Authorization	Type: hmac

Form data	{
	“base64hash”: “String”,
	“hashalg”: “String”
	}

Mô tả

TT	Tên biến	Kiểu	Mô tả

1	base64hash	String	Base64 của dữ liệu băm file PDF cần ký
2	hashalg	String	Thuật toán hàm băm: SHA1, SHA256, SHA512

Cấu trúc dữ liệu trả về

Trường	Dữ liệu
Header status	200 - Success, 401 Unauthorized , 404 - Not Found
Header Content-Type	application/json;charset=UTF-8

Form data	{
	“base64signature”: “String”,
	“status”: “int”,
	“description”: “String”
	}

Mô tả

TT	Tên biến	Kiểu	Mô tả
1	base64signature	String	Base64 của chữ ký giá trị băm file PDF
2	status	int	Mã lỗi của hàm ký số
3	description	String	Mô tả lỗi của hàm ký số

2.12. Ký file định dạng Office

Cấu trúc dữ liệu gửi lên

Trường	Dữ liệu
Request Method	POST
Request URL	http://10.0.15.164/api/office/sign/originaldata
Request Header Content-Type	application/json
Authorization	Type: hmac

Form data	{
	“base64office”: “String”,
	“hashalg”: “String”
	}

Mô tả

TT	Tên biến	Kiểu	Mô tả
1	base64office	String	Base64 của file PDF cần ký
2	hashalg	String	Thuật toán hàm băm: SHA1, SHA256, SHA512

Cấu trúc dữ liệu trả về

Trường	Dữ liệu
Header status	200 - Success, 401 Unauthorized , 404 - Not Found
Header Content-Type	application/json;charset=UTF-8

Form data	{
	“base64officeSigned”: “String”,
	“status”: “int”,
	“description”: “String”
	}

Mô tả

TT	Tên biến	Kiểu	Mô tả
1	base64officeSigned	String	Base64 của file Office đã có chữ ký
2	status	int	Mã lỗi của hàm ký số
3	description	String	Mô tả lỗi của hàm ký số

2.13. Ký hash file Office

Cấu trúc dữ liệu gửi lên

Trường	Dữ liệu
Request Method	POST
Request URL	http://10.0.15.164/api/office/sign/hashdata
Request Header Content-Type	application/json
Authorization	Type: hmac

Form data	{
	“base64digest”: “String”,
	“hashalg”: “String”
	}

Mô tả

TT	Tên biến	Kiểu	Mô tả
1	base64digest	String	Base64 của dữ liệu băm file office cần ký
2	hashalg	String	Thuật toán hàm băm: SHA1, SHA256, SHA512

Cấu trúc dữ liệu trả về

Trường	Dữ liệu
Header status	200 - Success, 401 Unauthorized , 404 - Not Found
Header Content-Type	application/json;charset=UTF-8

Form data	{
	“base64signature”: “String”,
	“keyInfoXml”: “String”,
	“status”: “int”,
	“description”: “String”
	}

Mô tả

TT	Tên biến	Kiểu	Mô tả

1	base64signature	String	Base64 của chữ ký giá trị băm file Office
2	keyInfoXml	String	Giá trị chứng thư số đã ký lên file
3	status	int	Mã lỗi của hàm ký số
4	description	String	Mô tả lỗi của hàm ký số

2.14. Ký file định dạng XML

Cấu trúc dữ liệu gửi lên

Trường	Dữ liệu
Request Method	POST
Request URL	http://10.0.15.164/api/xml/sign/defaultdata
Request Header Content-Type	application/json
Authorization	Type: hmac

Form data	{
	“base64xml”: “String”,
	“hashalg”: “String”
	}

Mô tả

TT	Tên biến	Kiểu	Mô tả
1	base64xml	String	Base64 của file xml cần ký
2	hashalg	String	Thuật toán hàm băm: SHA1, SHA256, SHA512

Cấu trúc dữ liệu trả về

Trường	Dữ liệu
Header status	200 - Success, 401 Unauthorized , 404 - Not Found
Header Content-Type	application/json;charset=UTF-8

Form data	{
	“base64xmlsigned”: “String”,
	“status”: “int”,
	“description”: “String”
	}

Mô tả

TT	Tên biến	Kiểu	Mô tả
1	base64xmlsigned	String	Base64 của file XML đã có chữ ký
2	status	int	Mã lỗi của hàm ký số
3	description	String	Mô tả lỗi của hàm ký số

2.15. Xác thực file Office

Cấu trúc dữ liệu gửi lên

Trường	Dữ liệu
Request Method	POST
Request URL	http://10.0.15.164/api/office/verify/hashdata
Request Header Content-Type	application/json
Authorization	Type: hmac

Form data	{
	“digest”: “String”,
	“algorithm”: “String”,
	“certificate”: “int”,
	“signature”: “String”
	}

Mô tả

TT	Tên biến	Kiểu	Mô tả

1	digest	String	Giá trị băm của file office
2	algorithm	String	Thuật toán sử dụng để ký số
3	certificate	String	Chứng thư số có trong file office
4	signature	String	Chữ ký của file office được ký

Cấu trúc dữ liệu trả về

Trường	Dữ liệu
Header status	200 - Success, 401 Unauthorized , 404 - Not Found
Header Content-Type	application/json;charset=UTF-8

Form data	{
	“resultCode”: “int”
	}

Mô tả

TT	Tên biến	Kiểu	Mô tả
1	resultCode	int	Kết quả xác thực chữ ký trên file office đã ký