CERTIGNA
a tessi solution

Spécifications du Webservice de signature

Edité le :	16 Avril 2021
Version :	2.0
Référence :	
Auteurs :	
Classification :	Confidentielle

tessi

Historique du document

Version	Date	Auteurs	Modifications apportées
1.0	14/12/2017	PMN	Création Refonte du Web Service - Utilisation du protocole REST
1.1	18/12/2017	PMN	Modification de la ressource signatures : changement nom variable + explication
1.2	09/01/2018	PMN	Intégration du format XAdES (signature enveloppante)
1.3	22/01/2018	PMN	Suppression de la ressource certificates. La sélection du certificat est faite en fonction du login (un certificat unique par login). Modification de la ressource signature pour intégration de la notion de signature visible Deux ressources distinctes pour la signature PAdES et XAdES
1.31	24/01/2018	PMN	Ajout précisions sur les coordonnées de la signature visible
1.32	31/01/2018	PMN	Signature visible : ajouts fonctionnalités suivantes • Gestion des numéros de page négatives • Gestion de la taille de la police du texte inséré (fixe ou proportionnelle à la taille du cadre)
1.4	10/09/2018	PMN	Ajout de la signature de hash
1.5	28/12/2018	PMN	Ajout du format CAdES
1.6	08/03/2019	PMN	Ajout du paramètre image dans la signature visible PadES
1.61	15/03/2019	PMN	Correction de l'URL du serveur de production (port standard 443 au lieu du port de pré-prod 1004)
2.0	16/04/2021	MV	Ajout signature avec certificat à la volée

Validation du document

Entité	Valideurs	Date
CERTIGNA	V.WYON	21/04/2021

SOMMAIRE

1 Introduction

1.1 Objet du document

Ce document décrit les fonctionnalités et la mise en œuvre des fonctions offertes par le service de signature développé et hébergé par DHIMYOTIS.

Ce service fonctionne en mode Client-Serveur et nécessite l'exploitation de l'API décrite dans le présent document.

La version actuelle du service couvre la signature des documents de type PDF en s'appuyant sur les standards :

- CAdES : CAdES-B, CAdES-T, CAdES-LT et CAdES-LTA (ETSI TS)
- PAdES : PAdES-B, PAdES-T, PAdES-LT et PAdES-LTA (ETSI TS)
- XAdES : XAdES-B, XAdES-T, XAdES-LT et XAdES-LTA (ETSI TS)

1.2 Connexion et Authentification

La connexion au service est sécurisée via le protocole SSL (https) à l'aide d'une authentification basique (entête HTTP Basic Authorization). Un identifiant et un mot de passe sont fournis à l'utilisateur lors de l'abonnement au service.

L'URL du service de pré-production est :
https://preprod-signature.dhimyotis.com:1004

L'URL du service de production est :
https://signature.dhimyotis.com/

1.3 Swagger

Une interface web est disponible permettant aux développeurs de tester les fonctionnalités de l'API sans avoir à développer quoi que ce soit. Cette interface accès au service de pré-production, un identifiant / mot de passe est donc nécessaire.

L'URL de ce service est :
https://swagger.certigna.com/signature/

1.4 Type de certificat de signature

Sur chaque point d'entrée, il est possible de signer à partir d'un certificat qui est soit :

- installé sur le serveur de signature : certificat cachet serveur émis pour l'entité utilisatrice du service ;
- fourni par l'appelant : certificat de type cachet serveur ou de type personne physique fourni sous forme de fichier PKCS#12 ;
- généré à la volée à partir de notre service de génération de certificat à la volée : les informations du signataire (Distinguished Name) doivent être fournis par l'appelant

2 FONCTIONNALITES

2.1 Signer un document au format PAdES

POST /api/v1/signature/pades

DESCRIPTION

Ce point d'entrée permet de signer un document PDF selon le standard PAdES (niveau B, T, LT et LTA). Il est possible de rendre visible la signature sur ce type de document.

Si le paramètre keyStore n'est pas fourni, alors la signature est effectuée avec un certificat Cachet Serveur de signature hébergé associé à votre compte.

PARAMETRES D'ENTETE

PARAMETRE	TYPE	DESCRIPTION
Authorization	String	Authentification Basique formatée comme suit : Basic *chaine_encodee_b64* chaine_encodee_base64 => chaine 'login:mot de passe' encodée en base64

PARAMETRES D'URL

Aucun paramètre

PARAMETRES DE REQUETE OBLIGATOIRES

PARAMETRE	TYPE	DESCRIPTION
digestAlgorithm	String	Algorithme de hashage compris dans la liste 'SHA256', 'SHA384', 'SHA512'
fileContent	String	Contenu du document encodé en base64
fileName	String	Nom du fichier
signatureLevel	String	Niveau de signature compris dans la liste : 'B', 'T', 'LT' ou 'LTA'

PARAMETRES DE REQUETE OPTIONNELS

PARAMETRE	TYPE	DESCRIPTION

keyStore	Structure	{
		type (string) : 'PKCS12KeyStore' (valeur fixe),
		password (string) : mot de passe du fichier PKCS#12,
		pkcs12Content (string) : contenu du fichier PKCS#12
		}

visibleSignature Parameters	Structure	{
		height (number) : la hauteur du cadre de signature (unité : point),
		width (number) : la largeur du cadre de signature (unité : point),
		x (number) : l'abscisse du coin supérieur gauche du cadre de signature,
		y (number) : l'ordonnée du coin supérieur gauche du cadre de signature,
		page (number) : le numéro de la page portant la signature visible,
		[- nbr pages, -1] U [1, nbr pages]
		imageParameters (structure) :
		{
		imageContent (string) : image encodée en base 64
		},
		textParameters (structure) :
		{
		fontSize (number) : taille de la police
		horizontalAlignment (string) : alignement horizontal ('CENTER, 'LEFT' ou 'RIGHT'),
		text (string) : texte à insérer
		}
		}

Concernant la signature visible :

- L'origine du référentiel (point de coordonnées (0,0)), se situe physiquement dans le coin haut gauche de la page. L'axe Y est orienté vers le bas, chaque point de la page a donc une abscisse et une ordonnée positives.

- La taille de la police est :
  - Valeur ‘0’ : taille proportionnelle au cadre de la signature visible
  - Autres valeurs (positives) : valeur de la taille de la police
- Le numéro de page est :
  - Valeur positive : numéro de page en commençant par le début du document
  - Valeur négative : numéro de page en commençant par la fin du document (-1 : dernière page, -2 : avant dernière page, etc.)
- Le retour chariot dans le champ text est symbolisé par le caractère ‘\n’

Une mise à l’échelle de l’image est effectuée pour être insérée exactement dans le cadre de la signature.

REPONSE

Le corps de la réponse contient le document signé.

Les codes HTTP renvoyés peuvent être :

200	Document signé
400	Mauvaise requête (un des champs requis n’a pas été fourni ou mal formaté)
401	Utilisateur non autorisé
500	Erreur interne de signature

EXEMPLE DE REQUETE

Signature PAdES invisible

```
curl -X POST --header 'Content-Type: application/json' -u "login:password"
-d '{"digestAlgorithm":"SHA256", "fileContent":"JVBERi0xLjE...yGC==",
"fileName":"monfichier.pdf", "signatureLevel":"LTA"}'
https://preprod-signature.dhimyotis.com:1004/api/v1/signature/pades
```

Signature PAdES visible

```
curl -X POST --header 'Content-Type: application/json' -u "login:password"
-d '{"digestAlgorithm":"SHA256", "fileContent":"JVBERi0xLjE...yGC==",
"fileName":"monfichier.pdf", "signatureLevel":"LTA",
"visibleSignatureParameters":{"height":100, "witdh":100, "x":0, "y":0,
"page":1, "textParameters":{"fontSize":10, "horizontalAlignment":"CENTER",
"text":"1ère ligne\n2nde ligne"}}}'
https://preprod-signature.dhimyotis.com:1004/api/v1/signature/pades
```

EXEMPLE DE DONNEES RETOURNEES

```
{
  "type": "PAdESResponse",
  "signedFileContent": "document signé encodé en base64"
}
```

2.2 Signer un document au format PAdES avec certificat à la volée

POST /v2/pades

DESCRIPTION

Ce point d'entrée permet de signer un document PDF selon le standard PAdES (niveau B, T, LT et LTA) à l'aide d'un certificat généré à la volée. Il est possible de rendre visible la signature sur ce type de document.

PARAMETRES D'ENTETE

PARAMETRE	TYPE	DESCRIPTION
Authorization	String	Authentification Basique formatée comme suit : Basic *chaine_encodee_b64* chaine_encodee_base64 => chaine 'login:mot de passe' encodée en base64
Content-type	String	application/json

PARAMETRES D'URL

Aucun paramètre

PARAMETRES DE REQUETE OBLIGATOIRES

PARAMETRE	TYPE	DESCRIPTION
digestAlgorithm	String	Algorithme de hashage compris dans la liste 'SHA256', 'SHA384', 'SHA512'
fileContent	String	Contenu du document encodé en base64
fileName	String	Nom du fichier
signatureLevel	String	Niveau de signature compris dans la liste : 'B', 'T', 'LT' ou 'LTA'
keyStore	Structure	*Si le signataire est un particulier :* { type (string) : 'PersonalOTFKeyStore' (valeur fixe), givenName (string) : prénom du signataire, surname (string) : nom du signataire, emailAddress (string) : email du signataire,

		countryName (string) : code pays sur 2 caractères (ISO 3166) / *optionnel*
		}
		Si le signataire est un professionnel :
		{
		type (string) : 'ProfessionalOTFKeyStore' (valeur fixe),
		givenName (string) : prénom du signataire,
		surname (string) : nom du signataire,
		emailAddress (string) : email du signataire,
		organizationalUnitName (string) : identifiant de l'entité,
		organizationName (strin) : nom de l'entité
		countryName (string) : code pays sur 2 caractères (ISO 3166) / *optionnel*
		}

PARAMETRES DE REQUETE OPTIONNELS

PARAMETRE	TYPE	DESCRIPTION
visibleSignature Parameters	Structure	{ height (number) : la hauteur du cadre de signature (unité : point), width (number) : la largeur du cadre de signature (unité : point), x (number) : l'abscisse du coin supérieur gauche du cadre de signature, y (number) : l'ordonnée du coin supérieur gauche du cadre de signature, page (number) : le numéro de la page portant la signature visible, [- nbr pages, -1] U [1, nbr pages] imageParameters (structure) : { imageContent (string) : image encodée en base 64 }, textParameters (structure) : { fontSize (number) : taille de la police

		horizontalAlignment (string) : alignement horizontal (‘CENTER, ‘LEFT’ ou ‘RIGHT’), text (string) : texte à insérer } }

Concernant la signature visible :

- L’origine du référentiel (point de coordonnées (0,0)), se situe physiquement dans le coin haut gauche de la page. L’axe Y est orienté vers le bas, chaque point de la page a donc une abscisse et une ordonnée positives.
- La taille de la police est :
  - Valeur ‘0’ : taille proportionnelle au cadre de la signature visible
  - Autres valeurs (positives) : valeur de la taille de la police
- Le numéro de page est :
  - Valeur positive : numéro de page en commençant par le début du document
  - Valeur négative : numéro de page en commençant par la fin du document (-1 : dernière page, -2 : avant dernière page, etc.)
- Le retour chariot dans le champ text est symbolisé par le caractère ‘\n’

Une mise à l’échelle de l’image est effectuée pour être insérée exactement dans le cadre de la signature.

REPONSE

Le corps de la réponse contient le document PDF signé.

Les codes HTTP renvoyés peuvent être :

200	Document signé
400	Mauvaise requête (un des champs requis n’a pas été fourni ou mal formaté)
401	Utilisateur non autorisé
500	Erreur interne de signature

EXEMPLE DE REQUETE

Signature PAdES avec un certif à la volée pour professionnel

```
curl -X POST --header 'Content-Type: application/json' -u "login:password"
-d '{"digestAlgorithm":"SHA384", "fileContent":"JVBERi0xLjE...yGC==",
"fileName":"monfichier.pdf", "signatureLevel":"B",
"keystore":{"type":"ProfessionalOTFKeyStore", "givenName":"User",
"surname":"TEST", "emailAddress":"em@domain.com",
"organizationalUnitName":"00000000000000", "organizationName":"MyCompany",
"countryName":"FR"}}'
https://preprod-signature.dhimyotis.com:1004/v2/pades
```

Signature PAdES avec un certif à la volée pour particulier

```
curl -X POST --header 'Content-Type: application/json' -u "login:password"
-d '{"digestAlgorithm":"SHA384", "fileContent":"JVBERi0xLjE...yGC==",
"fileName":"monfichier.pdf", "signatureLevel":"B",
"keystore":{"type":"PersonalOTFKeyStore", "givenName":"User",
"surname":"TEST", "emailAddress":"em@domain.com", "countryName":"FR"}}'
https://preprod-signature.dhimyotis.com:1004/v2/pades
```

EXEMPLE DE DONNEES RETOURNEES

```
{
  "type": "PAdESResponse",
  "signedFileContent": "document signé encodé en base64"
}
```

2.4 Signer un document au format XAdES

POST /api/v1/signature/xades

DESCRIPTION

Ce point d'entrée permet de signer un document selon le standard XAdES (niveau B, T, LT et LTA).

Si le paramètre keyStore n'est pas fourni, alors la signature est effectuée avec un certificat Cachet Serveur de signature hébergé associé à votre compte.

PARAMETRES D'ENTETE

PARAMETRE	TYPE	DESCRIPTION
Authorization	String	Authentification Basique formatée comme suit : Basic *chaine_encodee_b64* chaine_encodee_base64 => chaine 'login:mot de passe' encodée en base64
Content-type	String	application/json

PARAMETRES D'URL

Aucun paramètre

PARAMETRES DE REQUETE OBLIGATOIRES

PARAMETRE	TYPE	DESCRIPTION
digestAlgorithm	String	Algorithme de hashage compris dans la liste 'SHA256', 'SHA384', 'SHA512'
fileContent	String	Contenu du document encodé en base64
fileName	String	Nom du fichier
signatureLevel	String	Niveau de signature compris dans la liste : 'B', 'T', 'LT' ou 'LTA'
signaturePackaging	String	Type de signature compris dans la liste 'ENVELOPED' ou 'ENVELOPING'

PARAMETRES DE REQUETE OPTIONNELS

PARAMETRE	TYPE	DESCRIPTION

keyStore	Structure	{
		type (string) : 'PKCS12KeyStore' (valeur fixe),
		password (string) : mot de passe du fichier PKCS#12,
		pkcs12Content (string) : contenu du fichier PKCS#12
		}

REPONSE

Le corps de la réponse contient le document XAdES signé.

Les codes HTTP renvoyés peuvent être :

200	Document signé
400	Mauvaise requête (un des champs requis n'a pas été fourni ou mal formaté)
401	Utilisateur non autorisé
500	Erreur interne de signature
500	Erreur interne de signature

EXEMPLE DE REQUETE

```
curl -X POST --header 'Content-Type: application/json' -u "login:password"
-d '{"digestAlgorithm":"SHA256", "fileContent":"JVBERi0xLjE...yGC==",
"fileName":"monfichier.xml", "signatureLevel":"LTA",
"signaturePackaging":"ENVELOPED"}' https://preprod-
signature.dhimyotis.com:1004/api/v1/signature/xades
```

EXEMPLE DE DONNEES RETOURNEES

```
{
  "type": "XAdESResponse",
  "signedFileContent": "document signé encodé en base64"
}
```

2.5 Signer un document au format XAdES avec certificat à la volée

POST /v2/xades

DESCRIPTION

Ce point d'entrée permet de signer un document selon le standard XAdES (niveau B, T, LT et LTA) à l'aide d'un certificat généré à la volée.

PARAMETRES D'ENTETE

PARAMETRE	TYPE	DESCRIPTION
Authorization	String	Authentification Basique formatée comme suit : Basic *chaine_encodee_b64* chaine_encodee_base64 => chaine 'login:mot de passe' encodée en base64
Content-type	String	application/json

PARAMETRES D'URL

Aucun paramètre

PARAMETRES DE REQUETE OBLIGATOIRES

PARAMETRE	TYPE	DESCRIPTION
digestAlgorithm	String	Algorithme de hashage compris dans la liste 'SHA256', 'SHA384', 'SHA512'
fileContent	String	Contenu du document encodé en base64
fileName	String	Nom du fichier
signatureLevel	String	Niveau de signature compris dans la liste : 'B', 'T', 'LT' ou 'LTA'
signaturePackaging	String	Type de signature compris dans la liste 'ENVELOPED' ou 'ENVELOPING'
keyStore	Structure	*Si le signataire est un particulier :* { type (string) : 'PersonalOTFKeyStore' (valeur fixe), givenName (string) : prénom du signataire, surname (string) : nom du signataire,

		emailAddress (string) : email du signataire,
		countryName (string) : code pays sur 2 caractères (ISO 3166) / *optionnel*
		}
		Si le signataire est un professionnel :
		{
		type (string) : 'ProfessionalOTFKeyStore' (valeur fixe),
		givenName (string) : prénom du signataire,
		surname (string) : nom du signataire,
		emailAddress (string) : email du signataire,
		organizationalUnitName (string) : identifiant de l'entité,
		organizationName (strin) : nom de l'entité
		countryName (string) : code pays sur 2 caractères (ISO 3166) / *optionnel*
		}

REPONSE

Le corps de la réponse contient le document XAdES signé.

Les codes HTTP renvoyés peuvent être :

200	Document signé
400	Mauvaise requête (un des champs requis n'a pas été fourni ou mal formaté)
401	Utilisateur non autorisé
500	Erreur interne de signature

EXEMPLE DE REQUETE

```
curl -X POST --header 'Content-Type: application/json' -u "login:password"
-d '{"digestAlgorithm":"SHA256", "fileContent":"JVBERi0xLjE...yGC==",
"fileName":"monfichier.pdf", "signatureLevel":"LTA",
"signaturePackaging":"ENVELOPED",
"keystore":{"type":"ProfessionalOTFKeyStore", "givenName":"User",
"surname":"TEST", "emailAddress":"em@domain.com",
"organizationalUnitName":"00000000000000", "organizationName":"MyCompany",
"countryName":"FR"}}'
https://preprod-signature.dhimyotis.com:1004/v2/xades
```

EXEMPLE DE DONNEES RETOURNEES

```
{
  "type": "XAdESResponse",
  "signedFileContent": "document signé encodé en base64"
}
```

2.6 Signer un document au format CAdES

POST /api/v1/signature/cades

DESCRIPTION

Ce point d'entrée permet de signer un document selon le standard CAdES (niveau B, T, LT et LTA).

Si le paramètre keyStore n'est pas fourni, alors la signature est effectuée avec un certificat Cachet Serveur de signature hébergé associé à votre compte.

PARAMETRES D'ENTETE

PARAMETRE	TYPE	DESCRIPTION
Authorization	String	Authentification Basique formatée comme suit : Basic *chaine_encodee_b64* chaine_encodee_base64 => chaine 'login:mot de passe' encodée en base64
Content-type	String	application/json

PARAMETRES D'URL

Aucun paramètre

PARAMETRES DE REQUETE OBLIGATOIRES

PARAMETRE	TYPE	DESCRIPTION
digestAlgorithm	String	Algorithme de hashage compris dans la liste 'SHA256', 'SHA384', 'SHA512'
fileContent	String	Contenu du document encodé en base64
fileName	String	Nom du fichier
signatureLevel	String	Niveau de signature compris dans la liste : 'B', 'T', 'LT' ou 'LTA'
signaturePackaging	String	'ENVELOPING'

PARAMETRES DE REQUETE OPTIONNELS

PARAMETRE	TYPE	DESCRIPTION

keyStore	Structure	{
		type (string) : 'PKCS12KeyStore' (valeur fixe),
		password (string) : mot de passe du fichier PKCS#12,
		pkcs12Content (string) : contenu du fichier PKCS#12
		}

REPONSE

Le corps de la réponse contient le document CAdES signé.

Les codes HTTP renvoyés peuvent être :

200	Document signé
400	Mauvaise requête (un des champs requis n'a pas été fourni ou mal formaté)
401	Utilisateur non autorisé
500	Erreur interne de signature

EXEMPLE DE REQUETE

```
curl -X POST --header 'Content-Type: application/json' -u "login:password"
-d '{"digestAlgorithm":"SHA256", "fileContent":"JVBERi0xLjE...yGC==",
"fileName":"monfichier.pdf", "signatureLevel":"LTA",
"signaturePackaging":"ENVELOPING}'
https://preprod-signature.dhimyotis.com:1004/api/v1/signature/cades
```

EXEMPLE DE DONNEES RETOURNEES

```
{
  "type": "CAdESResponse",
  "signedFileContent": "document signé encodé en base64"
}
```

2.7 Signer un document au format CAdES avec certificat à la volée

POST /v2/cades

DESCRIPTION

Ce point d'entrée permet de signer un document selon le standard CAdES (niveau B, T, LT et LTA) à l'aide d'un certificat généré à la volée.

PARAMETRES D'ENTETE

PARAMETRE	TYPE	DESCRIPTION
Authorization	String	Authentification Basique formatée comme suit : Basic *chaine_encodee_b64* chaine_encodee_base64 => chaine 'login:mot de passe' encodée en base64
Content-type	String	application/json

PARAMETRES D'URL

Aucun paramètre

PARAMETRES DE REQUETE OBLIGATOIRES

PARAMETRE	TYPE	DESCRIPTION
digestAlgorithm	String	Algorithme de hashage compris dans la liste 'SHA256', 'SHA384', 'SHA512'
fileContent	String	Contenu du document encodé en base64
fileName	String	Nom du fichier
signatureLevel	String	Niveau de signature compris dans la liste : 'B', 'T', 'LT' ou 'LTA'
signaturePackaging	String	'ENVELOPING'
keyStore	Structure	*Si le signataire est un particulier :* { type (string) : 'PersonalOTFKeyStore' (valeur fixe), givenName (string) : prénom du signataire, surname (string) : nom du signataire, emailAddress (string) : email du signataire,

		countryName (string) : code pays sur 2 caractères (ISO 3166) / *optionnel*
		}
		Si le signataire est un professionnel :
		{
		type (string) : 'ProfessionalOTFKeyStore' (valeur fixe),
		givenName (string) : prénom du signataire,
		surname (string) : nom du signataire,
		emailAddress (string) : email du signataire,
		organizationalUnitName (string) : identifiant de l'entité,
		organizationName (strin) : nom de l'entité
		countryName (string) : code pays sur 2 caractères (ISO 3166) / *optionnel*
		}

REPONSE

Le corps de la réponse contient le document CAdES signé.

Les codes HTTP renvoyés peuvent être :

200	Document signé
400	Mauvaise requête (un des champs requis n'a pas été fourni ou mal formaté)
401	Utilisateur non autorisé
500	Erreur interne de signature

EXEMPLE DE REQUETE

```
curl -X POST --header 'Content-Type: application/json' -u "login:password"
-d '{"digestAlgorithm":"SHA256", "fileContent":"JVBERi0xLjE...yGC==",
"fileName":"monfichier", "signatureLevel":"LTA",
"signaturePackaging":"ENVELOPING",
"keystore":{"type":"PersonalOTFKeyStore", "givenName":"User",
"surname":"TEST", "emailAddress":"em@domain.com"}}'
https://preprod-signature.dhimyotis.com:1004/v2/cades
```

EXEMPLE DE DONNEES RETOURNEES

```
{
  "type": "CAdESResponse",
  "signedFileContent": "document signé encodé en base64"
}
```

2.8 Signer des empreintes numériques

POST /api/v1/signature/digest

DESCRIPTION

Ce point d'entrée permet de signer une ou plusieurs empreintes. Si la donnée privateKey n'est pas passée en paramètre, alors le service utilise le certificat configuré pour l'utilisateur connecté.

L'algorithme de hashage à utiliser pour générer les empreintes est à minima du SHA256. Il est de la responsabilité de l'appelant de générer l'empreinte des données à signer avant d'utiliser cette ressource. Celle-ci vérifie que le type de hashage passé en paramètre est autorisé.

La ressource vérifie également la cohérence du type d'algorithme avec la clé privée de signature (contrôle de cohérence de la longueur de l'empreinte avec celle du bloc de signature). Dans le cas des clés RSA 1024, 2048 ou 4096, les algorithmes de hachage autorisés sont SHA256, SHA384 et SHA512.

L'ordre des signatures correspond à celui des empreintes fournies dans la requête (l'empreinte et la signature correspondante sont stockées dans l'élément d'indice identique dans le tableau).

La réponse de l'API est un tout ou rien. En cas d'erreur de signature, il n'y a pas de réponse partielle remontée. Il est de la responsabilité de l'appelant de réitérer sa demande.

PARAMETRES D'ENTETE

PARAMETRE	TYPE	DESCRIPTION
Authorization	String	Authentification Basique formatée comme suit : Basic *chaine_encodee_b64* chaine_encodee_base64 => chaine 'login:mot de passe' encodée en base64
Content-type	String	application/json

PARAMETRES D'URL

Aucun paramètre

PARAMETRES DE REQUETE OBLIGATOIRES

PARAMETRE	TYPE	DESCRIPTION
digestAlgorithm	String	Valeur de l'algorithme de hash utilisé pour les empreintes (à minima SHA256)

digestValues	Array	Liste d'empreintes encodée chacune en base64 (maximum 20).

PARAMETRES DE REQUETE OPTIONNELS

PARAMETRE	TYPE	DESCRIPTION
privateKey	String	Clé privée au format PKCS#8, encodée en base 64

REPONSE

Le corps de la réponse contient le type d'algo de hash utilisé, le type de clé de signature (RSA ou ECDSA) et l'ensemble des signatures

Les codes HTTP renvoyés peuvent être :

200 Document signé
400 Mauvaise requête (un des champs requis n'a pas été fourni ou mal formaté)
401 Utilisateur non autorisé
500 Erreur interne de signature

EXEMPLE DE REQUETE

```
curl -X POST --header 'Content-Type: application/json' -u "login:password"
-d '{"digestAlgorithm":"SHA256", "digestValues":["JVBERi0xLjE...yGC==",
"XYkE...bvz=="]}'
https://preprod-signature.dhimyotis.com:1004/api/v1/signature/digest
```

EXEMPLE DE DONNEES RETOURNEES

```
{
  "type": "DigestSignatureResponse",
  "digestAlgorithm": "type d'algorithme de hashage passé en entrée",
  "encryptionAlgorithm": "RSA",
  "signatureValues": [
    "signature1 encodée en base64",
    "signature2 encodée en base64"
  ]
}
```

CERTIGNA

a tessi solution

www.certigna.com | www.dhimyotis.com

tessi