# CRYPTONEO
# -
# CONTRAT D'INTERFACE
# -
# API GÉNÉRIQUE DE SIGNATURE NUMÉRIQUE

## Autorité de Certification AC CRYPTONEO

**@CRYPTONEO - Novembre 2021**

## IDENTIFICATION DU DOCUMENT

| | |
|---|---|
| **NOM DU DOCUMENT** | SPÉCIFICATIONS DE L'API GÉNÉRIQUE DE SIGNATURE NUMÉRIQUE |
| **RÉFÉRENCE** | CPTN-API-GEN-SIGN-NUM-2021-11-22-MK-V1.0 |
| **CRÉATION** | CRYPTONEO / MARIUS KOUTOUAN |
| **DESTINATAIRES** | CRYPTONEO / ORANGE MALI / MAARCH |
| **DIFFUSION** | DIFFUSION CONTRÔLÉE |

## HISTORIQUE DU DOCUMENT

| VERSION | DATE | DESCRIPTION | RÉDACTION |
|---|---|---|---|
| 1.0 | 22/11/2021 | VERSION INITIALE | CRYPTONEO / MARIUS KOUTOUAN |



**CRYPTONEO** - ABIDJAN Cocody II Plateaux 7ème Tranche - Tel : (+225) 27.22.50.17.25 - 28 BP 657 Abidjan 28

Site Web : http://www.cryptoneo.com – Email : info@cryptoneo.com Compte Contribuable : 1516388V – Registre de Commerce : CI-ABJ-2014-B-19387

# Table des matières





**CRYPTONEO** - ABIDJAN Cocody II Plateaux 7ème Tranche - Tel : (+225) 27.22.50.17.25 - 28 BP 657 Abidjan 28
Site Web : http://www.cryptoneo.com – Email : info@cryptoneo.com
Compte Contribuable : 1516388V – Registre de Commerce : CI-ABJ-2014-B-19387

# 1. Objet du document

Ce document décrit la procédure à utiliser par un partenaire / intégrateur pour la consommation du service de signature numérique exposé par l'Autorité de Certification AC CRYPTONEO.

# 2. Liste des Interfaces

Pour la signature numérique de données numériques, 03 Services Web de type REST sont exposés :

| Ressource | Description |
|---|---|
| POST /authentification | Le end point d'obtention d'un jeton d'autorisation (token) JWT |
| POST /digitalSignature | Le end point de signature numérique |
| POST /certificateChain | Le end point de recuperation du certificat (clé publique) et de la chaine de certification |

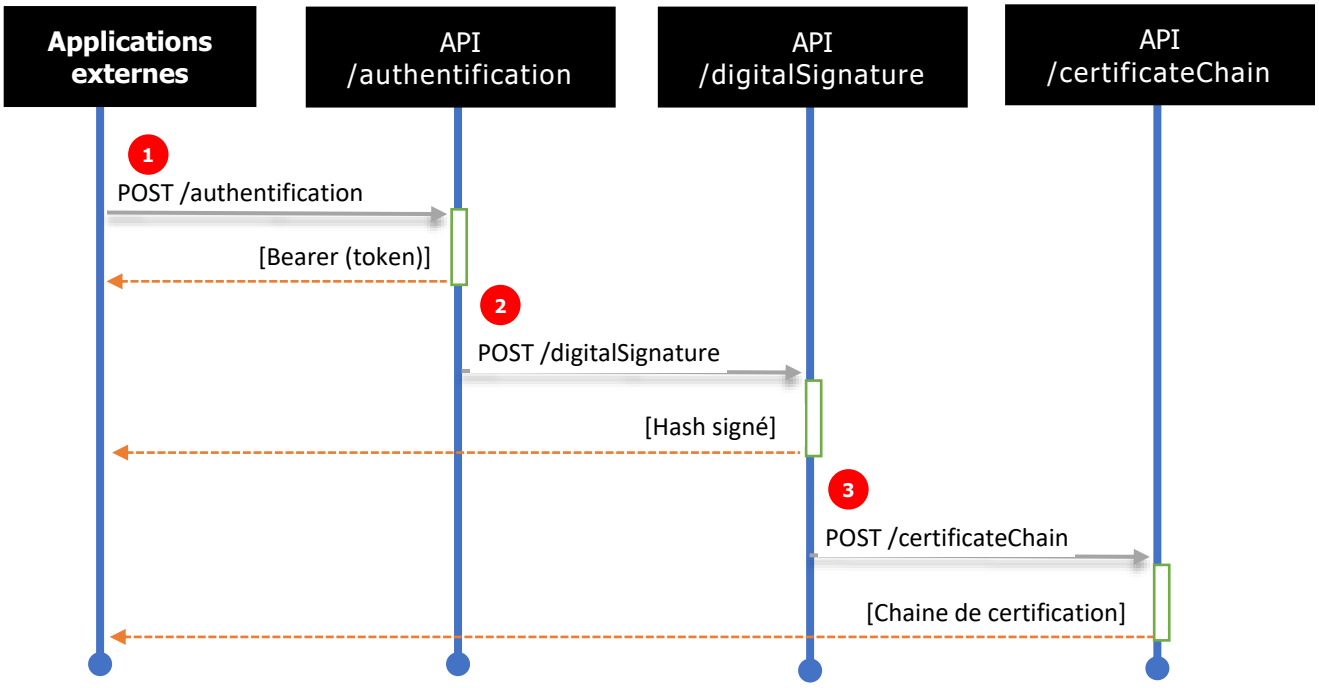
# 3. URL de Base

L'URL de base **[BASE_URL]** à utiliser pour l'accès aux ressources est :

***https://partners.cryptoneoplatforms.com/maarch/demo/digitalsignature***

# 4. Cinématique

Pour obtenir les données de signature numérique de l'empreinte d'une donnée numérique, les Web Services REST sont appelés dans l'ordre de séquencement ci-après :




**Description de la cinématique**

1- Le web service /authentification est appelé en premier, à chaque requête, pour s'authentifier.
2- Puis, le web Service /digitalSignature est appelé pour signer le Hash du document PDF.
3- Enfin, la chaine de certification est obtenue en consommant le web Service /certificateChain.



**CRYPTONEO** - ABIDJAN Cocody II Plateaux 7ème Tranche - Tel : (+225) 27.22.50.17.25 - 28 BP 657 Abidjan 28
Site Web : http://www.cryptoneo.com – Email : info@cryptoneo.com
Compte Contribuable : 1516388V – Registre de Commerce : CI-ABJ-2014-B-19387

# 5. Interfaces REST

## 5.1. Structure des Statuts de Réponses

| Key | Description | Format de la réponse |
|---|---|---|
| **statusCode** | Code de retour de la requête | **Application/Json** |
| **statusMessage** | Message de retour de la requête | |
| **data** | Données détaillées de retour de la plateforme de Signature numérique | |

## 5.2. Web Service « authentification »

### 5.2.1. Description

| Permet l'authentification sur la plateforme de signature numérique. | |
|---|---|
| **Méthode** | **Url** |
| POST | **[BASE_URL]**/authentification |

### 5.2.2. Requêtes

**Requête (Body)**

| Content-type | Paramètres | Type | Requis | Description | Commentaires |
|---|---|---|---|---|---|
| Application/Json | *login* | *String* | *Oui* | *Identifiant du compte d'authentification* | *Générés et transmis par CRYPTONEO* |
| | *password* | *String* | *Oui* | *Mot de passe du compte d'authentification* | |

Exemple de Requête Json

```
{
  "login": "Qs92HeTqjsdjfsfkbkbd53h6nF66r3cDQSJFVEZYKAMqFP5RdA4qg",
  "password": "c6jAzX33794BqezapouaW7wc7yReyU2tQM62KDLiqBHUSCBWbECa3Z73qxFCKt6j24"
}
```

### 5.2.3. Réponses Json

**Code de Succès**

| statusCode | statusMessage | Data | |
|---|---|---|---|
| | | ***Key*** | ***Value*** |
| 7001 | Opération réussie, Token obtenu. | token | *[Token JWT]* |

Exemple de Réponse Json

```
{
  "statusCode": 7001,
  "statusMessage": " Opération réussie, Token obtenu",
  "data":
        {
          "token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE1OTA2MTYxMjcsImV4cCI6MTU5MDYxODUyNywiY29"
        }
}
```



**CRYPTONEO** - ABIDJAN Cocody II Plateaux 7ème Tranche - Tel : (+225) 27.22.50.17.25 - 28 BP 657 Abidjan 28
Site Web : http://www.cryptoneo.com – Email : info@cryptoneo.com
Compte Contribuable : 1516388V – Registre de Commerce : CI-ABJ-2014-B-19387

## Codes d'Erreurs

| statusCode | statusMessage | data | |
|---|---|---|---|
| 8006 | Erreur, un ou plusieurs paramètres requis sont nuls ou invalides | *Liste détaillée de paramètre requis avec erreur* | |
| | | ***Key*** | ***Value*** |
| | | [Paramètre] | [Erreur] |

Exemple de Réponse Json

```
{
  "statusCode": 8006,
  "statusMessage": "Erreur, un ou plusieurs paramètres requis sont nuls ou invalides",
  "data":
        {
          "login": "doit être fourni et ne peut être null"
        }
}
```

| statusCode | statusMessage | data |
|---|---|---|
| 8007 | Authentification échouée, Login ou Mot de passe incorrect | null |

Exemple de Réponse Json

```
{
  "statusCode": 8007,
  "statusMessage": "Authentification échouée, Login ou Mot de passe incorrect",
  "data": null
}
```

| statusCode | statusMessage | data |
|---|---|---|
| 9000 | Impossible de traiter l'opération, veuillez contacter CRYPTONEO | null |

Exemple de Réponse Json

```
{
  "statusCode": 9000,
  "statusMessage": "Impossible de traiter l'opération, veuillez contacter Cryptoneo",
  "data": null
}
```



**CRYPTONEO** - ABIDJAN Cocody II Plateaux 7ème Tranche - Tel : (+225) 27.22.50.17.25 - 28 BP 657 Abidjan 28
Site Web : http://www.cryptoneo.com – Email : info@cryptoneo.com
Compte Contribuable : 1516388V – Registre de Commerce : CI-ABJ-2014-B-19387

## 5.3. Web Service « digitalSignature »

### 5.3.1. Description

| Permet de creer les données de signature numérique et signer l'empreinte de la donnée numérique. | |
|---|---|
| **Méthode** | **Url** |
| POST | **[BASE_URL]**/digitalSignature |

### 5.3.2. Requêtes

**Requête (Header)**

| Paramètres | Type | Requis | Description | Commentaires |
|---|---|---|---|---|
| **Berear [token]** | *Authorization* | *Oui* | **[token]** *Obtenu lors de l'authentification* | |

**Requête (Body)**

| Content-type | Paramètres | Type | Requis | Description | Commentaires |
|---|---|---|---|---|---|
| **application/octet-stream** | ***hashPdfToSign*** | *String* | *Oui* | *Valeur hashage du document à signer* | |
| | ***userName*** | *String* | *Oui* | *Valeur indiquant le Signataire du document* | |

Exemple de Requête Json

```
{
  " hashPdfToSign ": "MUswGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHATAkixIgQgUlDV\nkCHiLZB1HNtjPmq",
  " userName ": "mariusKOUTOUAN1418"
}
```

### 5.3.3. Réponses Json

**Code de Succès**

| statusCode | statusMessage | Data |
|---|---|---|
| 7000 | Opération réussie, Hash signé avec succès | ***[Hash signé]*** |

Exemple de Réponse Json

```
{
  " statusCode ": 7000,
  " statusMessage": "Opération réussie, Hash signé avec succès",
  "data": "TxwpSnSsiqjRwn2u1KUaolfXCWFdYJmIdTXRgVcwW3rWJsash1cgLF+KybCBe+xuw0BXmtI0UK2qgAeC
           q5UN9kytbj79w0pFnfKphMMmvl9bGoABvVu+WvPI3dMSncbqRdXMvl4khWp3j5UIe+2tzBBCjtIx5KMly
           gsJxw0oSizgDZJ0YkMMw8Z5bd8mHDqruq76mb7oouLCff/DarKBhZ7ea8ZFMb9iOOEnx81lotA3D0GaSK8Y
           8uBeArnRFZ6b5lpXqOfqSLbqyYZN0W29lIpU1a6XZ3EeFakGRAMPElpM9lE2LWlH+yYlA3suLirdgk7Ig1nY/R
           g5I77lHXlqZQ=="
}
```



**CRYPTONEO** - ABIDJAN Cocody II Plateaux 7ème Tranche - Tel : (+225) 27.22.50.17.25 - 28 BP 657 Abidjan 28
Site Web : http://www.cryptoneo.com – Email : info@cryptoneo.com
Compte Contribuable : 1516388V – Registre de Commerce : CI-ABJ-2014-B-19387

## Codes d'Erreurs

| statusCode | statusMessage | data |
|---|---|---|
| 8002 | Authentification échouée, le bearer doit être fourni | null |

Exemple de Réponse Json

```
{
  "statusCode": 8002,
  "statusMessage": "Authentification échouée, le bearer doit être fourni",
  "data": null
}
```

| statusCode | statusMessage | Data | |
|---|---|---|---|
| 8003 | Authentification échouée, le header d'autorisation est requis | *Liste détaillée de paramètre requis avec erreur* | |
| | | ***Key*** | ***Value*** |
| | | [Paramètre] | [Erreur] |

Exemple de Réponse Json

```
{
  "statusCode": 8003,
  "statusMessage": "Authentification échouée, le header d'autorisation est requis",
  "data":
        {
          "authorization": "Ce paramètre est requis dans le Header"
        }
}
```

| statusCode | statusMessage | Data | |
|---|---|---|---|
| 8006 | Erreur, un ou plusieurs paramètres requis sont nuls ou invalides | *Liste détaillée de paramètre requis avec erreur* | |
| | | ***Key*** | ***Value*** |
| | | [Paramètre] | [Erreur] |

Exemple de Réponse Json

```
{
  "statusCode": 8006,
  "statusMessage": " Erreur, un ou plusieurs paramètres requis sont nuls ou invalides",
  "data":
        {
          " userName ": "est requis et ne peut être null"
        }
}
```

| statusCode | statusMessage | data |
|---|---|---|
| 8012 | Session expirée, prendre un nouveau jeton d'authentification | null |

Exemple de Réponse Json

```
{
  "statusCode": 8012,
  "statusMessage": "Session expirée, prendre un nouveau jeton d'authentification",
  "data": null
}
```



**CRYPTONEO** - ABIDJAN Cocody II Plateaux 7ème Tranche - Tel : (+225) 27.22.50.17.25 - 28 BP 657 Abidjan 28
Site Web : http://www.cryptoneo.com – Email : info@cryptoneo.com
Compte Contribuable : 1516388V – Registre de Commerce : CI-ABJ-2014-B-19387

| statusCode | statusMessage | data |
|---|---|---|
| 9000 | Impossible de traiter l'opération, veuillez contacter Cryptoneo | null |

Exemple de Réponse Json

```
{
  "statusCode": 9000,
  "statusMessage": "Impossible de traiter l'opération, veuillez contacter Cryptoneo",
  "data": null
}
```

## 5.4. Web Service « certificateChain »

### 5.4.1. Description

| Permet de recuperer le certificat du signataire et la chaine de certification. | |
|---|---|
| **Méthode** | **Url** |
| POST | **[BASE_URL]** / certificateChain |

### 5.4.2. Requêtes

**Requête (Header)**

| Paramètres | Type | Requis | Description | Commentaires |
|---|---|---|---|---|
| **Berear [token]** | *Authorization* | *Oui* | **[token]** *Obtenu lors de l'authentification* | |

**Requête (Body)**

| Content-type | Paramètres | Type | Requis | Description | Commentaires |
|---|---|---|---|---|---|
| Application/Json | ***userName*** | *String* | *Oui* | *Valeur indiquant le Signataire du document* | *Fourni par CRYPTONEO* |
| | ***issuerdn*** | *String* | *Oui* | *DN du Certificat X.509* | *Fourni par CRYPTONEO* |
| | ***hexacertserialnumber*** | *String* | *Oui* | *Numero de série du Certificat* | *Fourni par CRYPTONEO* |

Exemple de Requête Json

```
{
  " userName ": "Yssouf TOURE",
  " issuerdn ": "CN=AC CRYPTONEO PERSONNES DEV ",
  " hexacertserialnumber": "28363efbbb713733",
}
```



**CRYPTONEO** - ABIDJAN Cocody II Plateaux 7ème Tranche - Tel : (+225) 27.22.50.17.25 - 28 BP 657 Abidjan 28
Site Web : http://www.cryptoneo.com – Email : info@cryptoneo.com
Compte Contribuable : 1516388V – Registre de Commerce : CI-ABJ-2014-B-19387

### 5.4.3. Réponses Json

**Code de Succès**

| statusCode | statusMessage | Data |
|---|---|---|
| 7002 | Opération réussie, Certificat récupéré avec succès | *[Hash signé]* |

Exemple de Réponse Json

```
{
  " statusCode ": 7002,
  " statusMessage ": "Opération réussie, Hash signé avec succès",
  "data": "TxwpSnSsiqjRwn2u1KUaolfXCWFdYJmIdTXRgVcwW3rWJsash1cgLF+KybCBe+xuw0BXmtI0UK2qg
           AeCq5UN9kytbj79w0pFnfKphMMmvl9bGoABvVu"
}
```

**Codes d'Erreurs**

| statusCode | statusMessage | data |
|---|---|---|
| 8002 | Authentification échouée, le bearer doit être fourni | null |

Exemple de Réponse Json

```
{
  "statusCode": 8002,
  "statusMessage": "Authentification échouée, le bearer doit être fourni",
  "data": null
}
```

| statusCode | statusMessage | Data | |
|---|---|---|---|
| 8003 | Authentification échouée, le header d'autorisation est requis | *Liste détaillée de paramètre requis avec erreur* | |
| | | *Key* | *Value* |
| | | [Paramètre] | [Erreur] |

Exemple de Réponse Json

```
{
  "statusCode": 8003,
  "statusMessage": "Authentification échouée, le header d'autorisation est requis",
  "data":
        {
          "authorization": "Ce paramètre est requis dans le Header"
        }
}
```



**CRYPTONEO** - ABIDJAN Cocody II Plateaux 7ème Tranche - Tel : (+225) 27.22.50.17.25 - 28 BP 657 Abidjan 28
Site Web : http://www.cryptoneo.com – Email : info@cryptoneo.com
Compte Contribuable : 1516388V – Registre de Commerce : CI-ABJ-2014-B-19387

| statusCode | statusMessage | Data | |
|---|---|---|---|
| 8006 | Erreur, un ou plusieurs paramètres requis sont nuls ou invalides | *Liste détaillée de paramètre requis avec erreur* | |
| | | ***Key*** | ***Value*** |
| | | [Paramètre] | [Erreur] |

Exemple de Réponse Json

```
{
  "statusCode": 8006,
  "statusMessage": " Erreur, un ou plusieurs paramètres requis sont nuls ou invalides",
  "data":
        {
          " userName ": "est requis et ne peut être null"
        }
}
```

| statusCode | statusMessage | data |
|---|---|---|
| 8012 | Session expirée, prendre un nouveau jeton d'authentification | null |

Exemple de Réponse Json

```
{
  "statusCode": 8012,
  "statusMessage": "Session expirée, prendre un nouveau jeton d'authentification",
  "data": null
}
```

| statusCode | statusMessage | data |
|---|---|---|
| 9000 | Impossible de traiter l'opération, veuillez contacter Cryptoneo | null |

Exemple de Réponse Json

```
{
  "statusCode": 9000,
  "statusMessage": "Impossible de traiter l'opération, veuillez contacter Cryptoneo",
  "data": null
}
```



**CRYPTONEO** - ABIDJAN Cocody II Plateaux 7ème Tranche - Tel : (+225) 27.22.50.17.25 - 28 BP 657 Abidjan 28
Site Web : http://www.cryptoneo.com – Email : info@cryptoneo.com
Compte Contribuable : 1516388V – Registre de Commerce : CI-ABJ-2014-B-19387

# 6. Liste Résumé des codes de retour

## Codes de Succès

| statusCode | statusMessage |
|---|---|
| 7000 | Opération réussie, Hash signé avec succès |
| 7001 | Opération réussie, Token obtenu |
| 7002 | Opération réussie, Certificat récupéré avec succès |

## Codes d'Erreurs

| statusCode | statusMessage |
|---|---|
| 8002 | Authentification échouée, le bearer doit être fourni |
| 8003 | Authentification échouée, le header d'autorisation est requis |
| 8006 | Erreur, un ou plusieurs paramètres requis sont nuls ou invalides |
| 8007 | Authentification échouée, Login ou Mot de passe incorrect |
| 8012 | Session expirée, prendre un nouveau jeton d'authentification |
| 9000 | Impossible de traiter l'opération, veuillez contacter Cryptoneo |
| 9006 | Échec relatif au Hash |



**CRYPTONEO** - ABIDJAN Cocody II Plateaux 7ème Tranche - Tel : (+225) 27.22.50.17.25 - 28 BP 657 Abidjan 28
Site Web : http://www.cryptoneo.com – Email : info@cryptoneo.com
Compte Contribuable : 1516388V – Registre de Commerce : CI-ABJ-2014-B-19387