MSC SSC (Servei Signatura Centralitzada)
API generació de signatures

Autor: **Roger Noguera i Arnau / OT PCI**
Data: **Gener 2025**

1. Introducció

Aquest document contempla les operacions de generació de signatures del Servei de Signatura Centralitzada.

⚠ La política d'autenticació de l'endpoint de `signatura` requereix presentar un certificat d'aplicació de l'ens a l'hora d'establir el canal HTTPS. Aquest certificat ha de ser vàlid i el CIF vinculat ha de correspondre amb el CIF de l'ens dipositari que realitza l'operació.

2. Creació de signatures

L'endpoint d'aquestes operacions a preproducció és el següent

```
https://cert.pci-cl-pre.aoc.cat/msc-ssc/api/signatura
https://pci-cl-pre.aoc.cat/msc-ssc/api/descarrega/<codi-signatura>
```

2.1 Signatures PDF

Elements		*Tipus*	*Descripció*
`dipositari`		string	INE10 de l'ens que realitza la signatura.
`rol`		string	CN del certificat carregat al SSC amb el que es realitzarà la signatura.
`pdf`	Bloc corresponent a la generació de signatura de PDF.		
	`forma`	string	Tipus de signatura: `PADES_T` (signatureAlgorithm *RSA_SHA256* i packaging *ENVELOPED*).
	`document`	Bloc corresponent al document PDF a signar. Per més detalls vegeu l'apartat 2.1.1 d'aquest document.	
	`parametres`	Bloc genèric per informar personalitzacions de la signatura (propietats de visibilitat, etc.). *TBD en funció dels usos reals dels clients externs (p.e. PCI no ho usa).*	

2.1.1 Document

Elements	*Tipus*	*Descripció*
`bytesB64`	string	Document a signar codificat en Base64.
`url`	string	Alternativament al document codificat en Base64 es pot informar una URL al document a signar (aquesta URL ha de ser accessible pel SSC). Adient per documents pesants.
`nom`	string	Nom del fitxer a signar.

```
{
    "dipositari": "9821920002",
    "rol": "Segell proves administracio electronica remot",
    "pdf": {
        "forma": "PADES_T",
        "document": {
            "bytesB64": "JVBERi0xLjMKJcT(...)SVFT0YK",
            "nom": "imprimible.pdf"
        }
    }
}
```

El servei té una restricció pel que fa a la grandària del cos del missatge de petició ja que els frontals estan configurats per no acceptar missatges de mida superior a 10MB. Tingueu-ho en compte a l'hora de passar documents grans codificats en base64 dins de l'element `bytesB64` (feu el pas per `url`).

2.2 Signatures XAdES

Elements			*Tipus*	*Descripció*
`dipositari`			string	INE10 de l'ens que realitza la signatura.
`rol`			string	CN del certificat carregat al SSC amb el que es realitzarà la signatura.
`xades`	Bloc corresponent a la generació de signatura XAdES.			
	`forma`		string	Tipus de signatura: `XADES_T`.
	`attached`	`document`	Bloc corresponent al document XML a signar. Per més detalls vegeu l'apartat 2.1.1 d'aquest document.	
		`packaging`	string	`ENVELOPED, ENVELOPING.`
		`signatureLocationXPath`	string	Opcional. XPath del XML a signar on s'incrustarà la signatura (només si `ENVELOPED`).

Elements			Tipus	Descripció
	detached	document	Bloc corresponent al document XML a signar. Per més detalls vegeu l'apartat 2.1.1 d'aquest document.	
		resum	Bloc corresponent al resum criptogràfic a signar. Per més detalls vegeu l'apartat 0 d'aquest document.	
	canonicalizationMethod		string	Opcional.
	digestAlgorithm		string	Opcional. `RSA_SHA1, RSA_SHA224, RSA_SHA256, RSA_SHA384, RSA_SHA512.`

- canonicalizationMethod:
  - http://www.w3.org/TR/2001/REC-xml-c14n-20010315
  - http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments
  - http://www.w3.org/2001/10/xml-exc-c14n#
  - http://www.w3.org/2001/10/xml-exc-c14n#WithComments
  - http://www.w3.org/2006/12/xml-c14n11
  - http://www.w3.org/2006/12/xml-c14n11#WithComments
  - http://santuario.apache.org/c14n/physical

```
{
    "dipositari": "9821920002",
    "rol": "Segell proves administracio electronica remot",
    "xades": {
        "forma": "XADES_T",
        "attached": {
            "document": {
                "bytesB64": "JVBERi0xLjMKJcTl8(...)VFT0YK"
            },
            "packaging": "ENVELOPING"
        }
    }
}
```

```
{
    "dipositari": "9821920002",
    "rol": "Segell proves administracio electronica remot",
    "xades": {
        "forma": "XADES_T",
        "detached": {
            "document": {
                "bytesB64": "JVBERi0xLjMKJcTl8(...)VFT0YK"
            }
        }
    }
}
```

```
{
    "dipositari": "9821920002",
    "rol": "Segell proves administracio electronica remot",
    "xades": {
        "forma": "XADES_T",
        "detached": {
            "resum": {
                "bytesB64": "02737e4e8c87d7466b623c1f844fdd71",
                "algorisme": "MD5"
            }
        }
    }
}
```

2.3 Signatures CAdES

Elements			*Tipus*	*Descripció*
`dipositari`			string	INE10 de l'ens que realitza la signatura.
`rol`			string	CN del certificat carregat al SSC amb el que es realitzarà la signatura.
`cades`	Bloc corresponent a la generació de signatura CAdES.			
	`forma`		string	Tipus de signatura: `CADES_T, CADES_B`. (signatureAlgorithm *RSA_SHA256* i si *attached*, packaging *ENVELOPED*).
	`attached`	`document`	Bloc corresponent al document a signar. Per més detalls vegeu l'apartat 2.1.1 d'aquest document.	
	`detached`	`document`		
		`resum`	Bloc corresponent al resum criptogràfic a signar. Per més detalls vegeu l'apartat 0 d'aquest document.	

```
{
    "dipositari": "9821920002",
    "rol": "Segell proves administracio electronica remot",
    "cades": {
        "forma": "CADES_T",
        "detached": {
            "document": {
                "bytesB64": "JVBERi0xLjMKJcTl8(...)VFT0YK"
            }
        }
    }
}
```

2.3.1 Resum

Elements	*Tipus*	*Descripció*
`bytesB64`	string	Resum criptogràfic a signar codificat en Base64.
`algorisme`	string	Algorisme emprat en la generació del resum criptogràfic a signar (`SHA1`, `SHA224`, `SHA256`, `SHA384`, `SHA512`, `RIPEMD160`, `MD2` i `MD5`).

2.4 Xifrat d'un resum

Elements			*Tipus*	*Descripció*
`dipositari`			string	INE10 de l'ens que realitza la signatura.
`rol`			string	CN del certificat carregat al SSC amb el que es realitzarà la signatura.
`pkcs1`	Bloc corresponent a la generació del xifrat d'un resum segons l'estàndard criptogràfic de clau pública PKCS1. (signatureAlgorithm *RSA_SHA256*, algorisme de xifrat *RSA* i algorisme de resum *SHA256*).			
	`resum`	`bytesB64`		Resum criptogràfic (SHA-256) a xifrar codificat en Base64.

```
{
    "dipositari": "9821920002",
    "rol": "Segell proves administracio electronica remot",
    "pkcs1": {
        "resum": {
            "bytesB64": vQWXEnH2tO5710sDQMUtfau/09bxi8VpR4O7vdCZKCs="
        }
    }
}
```

3. Resposta de creació de signatura

Elements		*Tipus*	*Descripció*
`resultat`	Bloc de dades corresponent al resultat de l'operació.		
	`codi`	string	Codi de resultat de l'operació: • `0`: signatura realitzada correctament. • `0502`: error realitzant l'operació
	`descripcio`	string	Descripció del resultat de l'operació.
`signatura`	Bloc de dades corresponent a la signatura generada.		
	`bytesB64`	string	Bloc de dades corresponent a la signatura generada. En documents lleugers informa

Elements		*Tipus*	*Descripció*
			l'element `bytesB64` però en documents pesants s'ha d'obtenir via descàrrega amb el `codi` de signatura.
	`codi`	string	Codi de signatura per realitzar la descàrrega (no aplica al xifrat de resums).

```
-- Exemple: signatura d'un document / resum.

{
    "signatura": {
        "bytesB64": " JVBERi0xLjMKJcT(...)SVFT0YK"
        "codi": "QHD7-LOAC-OF2O-TC3Q-L174-0128-5193-31"
    },
    "resultat": {
        "codi": "0",
        "descripcio": "Operació realitzada correctament"
    }
}
```

```
-- Exemple: signatura d'un document pesant.

{
    "signatura": {
        "codi": "QHD7-LOAC-OF2O-TC3Q-L174-0128-5193-31"
    },
    "resultat": {
        "codi": "0",
        "descripcio": "Operació realitzada correctament"
    }
```

4. Comprovació de disponibilitat d'un certificat

L'endpoint d'aquesta operació a preproducció és el següent

```
https://cert.pci-cl-pre.aoc.cat/msc-ssc/api/validar-rol
```

Elements	*Tipus*	*Descripció*
`dipositari`	string	INE10 de l'ens dipositari
`rol`	string	CN del certificat carregat al SSC que es vol validar l'existència.

```
{
    "dipositari": "9821920002",
    "rol": "Segell proves administracio electronica remot"
}
```

Elements		*Tipus*	*Descripció*
`resultat`	Bloc de dades corresponent al resultat de l'operació.		
	`codi`	string	Codi de resultat de l'operació: • `0`: consta. • `1`: no consta. • `0502`: error realitzant l'operació
	`descripcio`	string	Descripció del resultat de l'operació.
`caducitat`		string	Si consta, data de caducitat del certificat (`DD-MM-AAAA HH24:MI:SS`).

```
{
    "resultat": {
        "codi": "0",
        "descripcio": "Consta"
    },
    "caducitat": "27-01-2029 10:01:24"
}
```