

## **GATEFIRE**

### **GATEWAY DI FIRMA DIGITALE E REPOSITORY**

#### **018:Apposizione firma digitale massiva CADES**

**Versione 1.0**

## INDICE

1.	Obiettivi	3
1.1	Scopo del servizio	3
2.	Fruitori	3
3.	Contesto	3
4.	Modalità di richiamo	3
5.	Descrizione delle operazioni del servizio di firma digitale massiva	3
5.1	Interfaccia di richiamo (input)	3
5.2	Interfaccia di output con Codice esito = 0 (ok)	6
5.3	Interfaccia di output con Codice esito $\neq$ 0 (Nok)	7
5.4	Tipologie di interfaccia richieste	9

## 1. Obiettivi

### 1.1 Scopo del servizio

Il metodo **firmaCADESMassiva** del Web Service **GateFireSrvc** permette di apporre una firma digitale in modalità remota o automatica (nel seguito indicate rispettivamente come firma remota o firma automatica), di tipo CADES ad un gruppo di file, in modo simultaneo.

Questo metodo firma utilizzando la Certification Authority richiesta dall'applicativo chiamante.

## 2. Fruitori

I fruitori del servizio sono gli applicativi verticali che passano a Gatefire il file da firmare digitalmente.

## 3. Contesto

Non trattandosi di un sistema particolarmente complesso, non si ritiene utile fornire una visione di sintesi del contesto a cui il servizio si riferisce.

## 4. Modalità di richiamo

Il servizio viene richiamato con modalità sincrona.

## 5. Descrizione delle operazioni del servizio di firma digitale massiva

A fronte dell'esecuzione del servizio da parte di una applicazione chiamante, il servizio stesso esegue l'apposizione massiva della firma digitale su più file, utilizzando i servizi messi a disposizione dalla CA anch'essa indicata dall'applicazione chiamante.

Il servizio necessita:

- di un otp che permette di determinare se verrà utilizzato il servizio di firma massiva remota (**firmaCADESMassivaRemota**) o automatica (**firmaCADESMassivaAutomatica**)
- delle credenziali di firma dell'utente (alias e pin)

Il servizio restituisce un file zip contenente tutti i file firmati. **Qualora anche un solo file non venisse firmato a causa di un errore, il file zip viene restituito vuoto.**

### 5.1 Interfaccia di richiamo (input)

Struttura:

```
<soapenv:Envelope
```

```
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:gat="http://www.csi.it/gatefire/">
```

```
<soapenv:Header/>
```

```
<soapenv:Body>
```

```
<gat:firmaCADESMassiva>
```

```
<attachment>
```

```
<file>cid:398244124816</file>
```

```
<fileName>ordinativo_non_firmato1.xml</fileName>
```

```
</attachment>
```

```
<attachment>
```

```
<file>cid:398244124816</file>
```

```
<fileName>ordinativo_non_firmato2.xml</fileName>
</attachment>
<caDesInput>
  <callInfo>
    <applicationCode>NOME_APPLICAZIONE</applicationCode>
    <caCode>INFOCERT</caCode>
    <codiceFiscale>xxxxxxxxxx</codiceFiscale>
    <collocazione>010666</collocazione>
  </callInfo>
  <requiredMark>false</requiredMark>
</caDesInput>
<identity>
  <password>xxxx</password>
  <user>xxxxx</user>
</identity>
</gat:firmaCAAdESMassiva>
</soapenv:Body>
</soapenv:Envelope>
```

#### Descrizione delle sezioni

- **attachment:** (sezione ripetuta) contiene i file da firmare
- **identity:** contiene le credenziali di firma
  - *user*
  - *password*
  - *otp*: se specificato viene chiamato il servizio per la firma massiva remota, altrimenti quello per la firma massiva automatica
- **caDesInput:**
  - *requiredMark*: indica se oltre alla firma e' necessaria anche la marcatura temporale
  - *markIdentity*: credenziali per la marca temporale (solo se requiredMark=true)
  - *callInfo*: contiene i dettagli dell'utente chiamante
    - *applicationCode* (obbligatorio, codice del verticale chiamante es. ESENPAT)
    - *caCode* (INFOCERT o ARUBA)
    - *codiceFiscale*
    - *collocazione* (obbligatorio identificativo ASL chiamante, es per TO5 utilizzare il codice 010205)
    - *dominio* (opzionale. necessario solo se una *collocazione* ha più domini configurati per quel tipo di firma)

Informazione di input	Riferimento (Entità.attributo)	Obbligatorio	Esempio
files da firmare	Sezione ripetibile <attachment> <file>?</file> <fileName>?</fileName>	Si	
otp	Sezione <identity> <otp>?</otp>	No Se presente indica firma digitale REMOTA, Se assente indica firma digitale AUTOMATICA	<otp>1234567890</otp> (può essere ricavato utilizzando il servizio a disposizione)
user_id (delle credenziali CA)	Sezione <identity> <user>?</user>	Si	
password (delle credenziali CA)	Sezione <identity> <password>?</password>	Si	
codice CA	Sezione <caInput><callInfo> <caCode>?</caCode>	Si Vale ARUBA o INFOCERT	<caCode>INFOCERT</caCode>
codice applicazione chiamante	Sezione <caInput><callInfo> <applicationCode>?</applicatio nCode>	Si Deve essere il codice di uno dei verticali configurati	<applicationCode>EENPAT</applicatio nCode>
codice fiscale utente	Sezione <caInput><callInfo> <codiceFiscale>?</codiceFiscal e>	Si	<codiceFiscale>BCDFGH70L01D969X</ codiceFiscale>
collocazione	Sezione <caInput><callInfo> <collocazione>?</collocazione >	Si Deve essere una delle collocazioni configurate	<collocazione>010205</collocazione>
dominio	Sezione <caInput><callInfo> <dominio>?</dominio>	No Ricavato dalla configurazione se non specificato	Obbligatorio se esistono più domini di firma per la collocazione passata in input
richiesta marcatura	Sezione <caInput> <requiredMark>false</required Mark>	Si Sempre “false”	<requiredMark>false</requiredMark>

**Esempio:**

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:gat="http://www.csi.it/gatefire/">
  <soapenv:Header/>
  <soapenv:Body>
    <gat:firmaCADESMassiva>
      <attachment>
        <file>cid:398244124816</file>
        <fileName>ordinativo_non_firmato1.xml</fileName>
      </attachment>
      <attachment>
        <file>cid:398244124816</file>
        <fileName>ordinativo_non_firmato2.xml</fileName>
      </attachment>
      <caDesInput>
        <callInfo>
          <applicationCode>NOME_APPLICAZIONE</applicationCode>
          <caCode>INFOCERT</caCode>
          <codiceFiscale>xxxxxxxxxx</codiceFiscale>
          <collocazione>010666</collocazione>
        </callInfo>
        <requiredMark>false</requiredMark>
      </caDesInput>
      <identity>
        <password>xxxx</password>
        <user>xxxxx</user>
      </identity>
    </gat:firmaCADESMassiva>
  </soapenv:Body>
</soapenv:Envelope>
```

## 5.2 Interfaccia di output con errorCode = 0 (ok)

Struttura:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ns2:firmaCADESMassivaResponse xmlns:ns2="http://www.csi.it/gatefire/">
      <return>
        <result>
          <errorCode>0</errorCode>
        </result>
        <attachment>
          <file>?</file>
          <fileName>?</fileName>
        </attachment>
      </return>
    </ns2:firmaCADESMassivaResponse>
  </soap:Body>
```

</soap:Envelope>

Informazione di output	Riferimento (Entità.attributo)
codice di errore	Sezione <result> <errorCode>?</errorCode>
Zip contenente i file firmati (contenuto e nome del file .zip)	Sezione <attachment> <file>?</file> <fileName>?</fileName>

### 5.3 Interfaccia di output con errorCode <> 0 (Nok)

Struttura:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ns2:firmaCAAdESMassivaResponse xmlns:ns2="http://www.csi.it/gatefire/">
      <return>
        <result>
          <description>?</description>
          <errorCode>?</errorCode>
          <message>?</message>
          <originalReturnCode>?</originalReturnCode>
        </result>
      </return>
    </ns2:firmaCAAdESMassivaResponse>
  </soap:Body>
</soap:Envelope>
```

Informazione di output	Riferimento (Entità.attributo)
codice di errore gatefire	Sezione <result> <errorCode>?</errorCode>
descrizione dell'errore gatefire	Sezione <result> <description>?</description>
descrizione dettagliata dell'errore (se presente descrizione estesa della CA)	Sezione <result> <message>?</message>
codice di errore restituito dalla CA	Sezione <result> <originalReturnCode>?</originalReturnCode>

### Esempi di codici e descrizioni di errore

Codice	Descrizione Sintetica	Descrizione Estesa	Nota
100	Mancata connessione al DB	Problemi di comunicazione con il DB di Gatefire	
101	Mancata connessione alla CA	Problemi di comunicazione con la CA selezionata	

200	Parametri obbligatori mancanti	Parametri obbligatori non presenti	Il tag <message> contiene il dettaglio dei parametri in errore
201	CA selezionata non valida	La CA selezionata non è presente tra le CA gestite da Gatefire	
202	Codice Fiscale errato	Il codice fiscale non è formalmente corretto	
203	Dimensione del file non valida	Il file ha dimensione pari a zero o superiore alla dimensione massima prevista	
204	Credenziali non valide	Le credenziali fornite per la CA non sono valide	
206	Numero file in input supera il limite previsto	Il numero dei file passato in input è superiore al limite massimo previsto	
207	Dimensione dei file in input supera il limite previsto	La dimensione complessiva dei file passati in punti supera i limiti consentiti	
208	Errore apposizione firma	Il servizio di apposizione della firma ha restituito un errore	Errore durante la chiamata alla CA o restituito direttamente dalla CA. Il tag <originalReturnCode> contiene il codice di errore restituito dalla CA (vedi tabella successiva).
500	Errore generico	Tutti gli altri errori non esplicitamente definiti/gestiti	Il tag <message> contiene il dettaglio dell'errore (es problemi di rete, filesystem, ecc.)

#### Esempi di codici di errore restituiti dalla CA

CA	Codice	Descrizione
Aruba	0001	Errore generico nel processo di firma
	0002	Parametri non corretti per il tipo di trasporto indicato
	0003	Errore in fase di verifica delle credenziali
	0004	Errore nel PIN
	0005	Tipo di trasporto non valido
	0006	Tipo di trasporto non autorizzato
	0007	Profilo Di firma non valido
	0008	Impossibile completare l'operazione di marcatura temporale (es irraggiungibilità del servizio, marche residue terminate, etc..)
	0009	Credenziali di delega non valide
	0010	Lo stato dell'utente non è valido (es. utente sospeso)
Infocert	PRS-0000	Errore sconosciuto
	PRS-0001	Formato del pin errato, deve essere numerico e di 8 cifre
	PRS-0002	L'alias fornito non ha un certificato valido



	PRS-0003	L'alias fornito è bloccato per troppi tentativi di inserimento pin errati
	PRS-0005	L'alias fornito ha il certificato scaduto
	PRS-0006	OTP non specificato
	PRS-0007	Parametri mancanti
	PRS-0008	Errore di comunicazione con il server di firma
	PRS-0010	L'alias fornito non ha un nessun certificato in stato evaso
	PRS-0011	L'alias o pin errati
	PRS-0012	Tipologia di firma errata
	PRS-0014	Non è stato fornito il pin
	PRS-0015	Errore interno del server di firma
	PRS-0016	L'OTP inserito non è corretto
	PRS-0018	Pin errato
	PRS-0019	Alias non trovato
	PRS-0020	Errore durante la ricerca dell'alias
	PRS-0021	Errore durante la generazione della marca
	PRS-0024	Errore durante l'upload del file
	PRS-0027	Il content type del file inviato non è corretto

#### **5.4 Tipologie di interfaccia richieste**

È prevista l'interfacciamento verso i seguenti sistemi:

- CA Aruba
- CA Infocert