

GATEFIRE

GATEWAY DI FIRMA DIGITALE E REPOSITORY

024:Apposizione firma digitale CADES

Versione 2.0

VERS.	PARAGRAFO O PAGINA	DESCRIZIONE DELLA VARIAZIONE
2.0	Paragrafi 5.2.1, 5.4.1, 5.5	Aggiunta UANATACA come CA

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	3
5.1	Invocazione del servizio di firma digitale	3
5.1.1	Descrizione dell'operazione	3
5.2	Interfaccia di richiamo (input)	4
5.2.1	Metodo firmaCADES	4
5.3	Interfaccia di output con Codice esito = 0 (ok)	7
5.4	Interfaccia di output con Codice esito $\neq$ 0 (Nok)	8
5.4.1	Codici di errore	9
5.5	Tipologie di interfaccia richieste	10

1. Obiettivi

1.1 Scopo del servizio

Il metodo **firmaCADES** del Web Service **GateFireSrv** permette di apporre una firma digitale in modalità remota o automatica (nel seguito indicate rispettivamente come firma remota o firma automatica), di tipo CADES. Questi metodi firmano utilizzando la Certification Authority richiesta dall'applicativo chiamante.

2. Fruitore

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

A fronte dell'esecuzione del servizio da parte di una applicazione chiamante, il servizio stesso esegue l'apposizione della firma digitale sul file di tipo xml, 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 remota (**firmaCADESRemota**) o automatica (**firmaCADESAutomatica**)
- delle credenziali della CA dell'utente (alias e pin)

5.1 Invocazione del servizio di firma digitale

5.1.1 Descrizione dell'operazione

Il metodo **firmaCades** invoca l'esecuzione del servizio di apposizione della firma digitale (remota o automatica) al file passato in input dall'applicativo chiamante.

Il metodo utilizza l'apposito servizio messo a disposizione dalla CA anch'essa passata dall'applicativo chiamante sotto forma di parametro.

In base alla presenza del parametro otp il metodo chiama il servizio corrispondente:

- se otp presente viene invocato il servizio **firmaCadesRemota** per l'apposizione della firma digitale remota
- se otp assente viene invocato il servizio **firmaCadesAutomatica** per l'apposizione della firma digitale automatica

Il servizio di firma digitale restituisce il file firmato in base alla tipologia richiesta e uno stato di esito dell'operazione eseguita.

In caso di errore di interfacciamento con sistemi CA: si va alla terminazione del servizio con esito ERRORE.

5.2 Interfaccia di richiamo (input)

5.2.1 Metodo firmaCADES

Struttura:

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:gat="http://www.csi.it/gatefire/">
  <soapenv:Header/>
  <soapenv:Body>
    <gat:firmaCADES>
      <attachment>
        <file>cid:1461656719233</file>
        <fileName>ordinativo_non_firmato.xml</fileName>
      </attachment>
      <caDesInput>
        <callInfo>
          <applicationCode>NOME_APPLICAZIONE</applicationCode>
          <caCode>INFOCERT</caCode>
          <codiceFiscale>XXXXXXXXXXXXXXXXXX</codiceFiscale>
          <collocazione>010666</collocazione>
        </callInfo>
        <markIdentity>
          <!--Optional:-->
          <password>?</password>
          <!--Optional:-->
          <user>?</user>
        </markIdentity>
        <requiredMark>>false</requiredMark>
        <xpath></xpath>
      </caDesInput>
      <identity>
        <!--Optional:-->
        <otp>?</otp>
        <password>xxxxx</password>
        <user>xxxxxx</user>
      </identity>
    </gat:firmaCADES>
  </soapenv:Body>
</soapenv:Envelope>
```

Descrizione delle sezioni

- **attachment:** contiene il file da firmare
 - **identity:** contiene le credenziali di firma
 - *user*
 - *password*
 - *otp*: se specificato viene chiamato il servizio per la firma remota, altrimenti quello per la firma automatica
- per UANATACA contiene le credenziali di firma:

- *alias*
 - *password*
 - *pin*
 - *otp*: se specificato viene chiamato il servizio per la firma remota, altrimenti quello per la firma 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* (obbligatorio INFOCERT, ARUBA o UANATACA)
 - *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
file da firmare	Sezione <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	
Pin	Sezione <identity> <pin>?</ pin >	Si Vale per UANATACA	<pin>1234</ pin >
codice CA	Sezione <caInput><callInfo> <caCode>?</caCode>	Si Vale ARUBA, INFOCERT o UANATACA	<caCode>INFOCERT</caCode>
codice applicazione chiamante	Sezione <caInput><callInfo> <applicationCode>?</applicatio nCode>	Si Deve essere il codice di uno dei verticali configurati	<applicationCode>ESENPA</a pplicationCode>
codice fiscale utente	Sezione <caInput><callInfo> <codiceFiscale>?</codiceFiscal e>	Si	<codiceFiscale>BCDFGH70L01 D969X</codiceFiscale>
collocazione	Sezione <caInput><callInfo> <collocazione>?</collocazione >	Si Deve essere una delle collocazioni configurate	<collocazione>010205</collocaz ione>
dominio	Sezione <caInput><callInfo> <dominio>?</dominio>	No Ricavato dalla configurazione se non specificato	
richiesta marcatura	Sezione < caInput > <requiredMark>false</required Mark>	Si Sempre “false”	<requiredMark>false</requiredM ark>

Esempio:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:gat="http://www.csi.it/gatefire/">
  <soapenv:Header/>
  <soapenv:Body>
    <gat:firmaCADES>
      <!--Optional:-->
      <attachment>
        <!--Optional:-->
        <file>cid:679643644086</file>
        <!--Optional:-->
        <fileName>Immagine_2023-09-25 171437.png</fileName>
      </attachment>
      <!--Optional:-->
      <caDesInput>
        <!--Optional:-->
        <callInfo>
          <applicationCode>ESENPAT</applicationCode>
          <caCode>INFOCERT</caCode>
          <codiceFiscale>MNTRFLXXM46CXXX</codiceFiscale>
          <collocazione>010666</collocazione>
        </callInfo>
        <requiredMark>false</requiredMark>
      </caDesInput>
      <!--Optional:-->
      <identity>
        <password>123XXX</password>
        <user>PROXY_SIGN_EXAMPLE</user>
      </identity>
    </gat:firmaCADES>
  </soapenv:Body>
</soapenv:Envelope>
```

5.3 Interfaccia di output con Codice esito = 0 (ok)

Struttura:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ns3:firmaCADESResponse
xmlns:xds="http://www.openehealth.org/ipf/xds" xmlns:ns3="http://www.csi.it/gatefire/">
      <return>
        <result>
          <errorCode>0</errorCode>
        </result>
        <attachment>
          <file>base64_file_firmato </file>
```

```
<fileName> 308c82df-efd3-451f-849b-b7d5e4d3d63b. png </fileName>
</attachment>
</return>
</ns3:firmaCAAdESResponse>
</soap:Body>
</soap:Envelope>
```

Informazione di output	Riferimento (Entità.attributo)
codice di errore	Sezione <result> <errorCode>?</errorCode>
File firmato (contenuto)	Sezione <attachment> <file>?</file>
filename (nome del file firmato)	<fileName> </fileName>

5.4 Interfaccia di output con Codice esito <> 0 (Nok)

Struttura:

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

	GATEFIRE-GATEWAY DI FIRMA DIGITALE E REPOSITORY SPECIFICA SERVIZIO 024 APPOSIZIONE FIRMA DIGITALE CADES	GATEFIRE—SER-024 Pag. 9 di 10
---	--	---

Informazione di output	Riferimento (Entità.attributo)
	<originalReturnCode>?</originalReturnCode>

5.4.1 Codici di errore

Esempi di codici e descrizioni di errore

Status	Code	Title	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	
208	Errore apposizione firma	Il servizio di apposizione della firma ha restituito un errore (con indicazione del messaggio di 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..)
	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
Uanataca	401	Utente non autorizzato
	422	Request errata

5.5 Tipologie di interfaccia richieste

È previsto l'interfacciamento verso i seguenti sistemi:

- CA Aruba
- CA Infocert
- CA Uanataca