

|                                                                                   |                                                                                                                                |                                      |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
|  | <b>GATEFIRE-GATEWAY DI FIRMA<br/>DIGITALE E REPOSITORY<br/>SPECIFICA SERVIZIO<br/>016 APPOSIZIONE FIRMA DIGITALE<br/>XADES</b> | GATEFIRE—SER-016<br><br>Pag. 1 di 11 |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|

# GATEFIRE

## GATEWAY DI FIRMA DIGITALE E REPOSITORY

### 016:Apposizione firma digitale XADES

**Versione 2.0**

#### STATO DELLE VARIAZIONI

| VERS. | PARAGRAFO O<br>PAGINA      | DESCRIZIONE DELLA VARIAZIONE |
|-------|----------------------------|------------------------------|
| 2.0   | Paragrafi 5.1, 5.3.2 e 5.4 | Aggiunta UANATACA come CA    |

|                                                                                   |                                                                                                                                |                                      |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
|  | <b>GATEFIRE-GATEWAY DI FIRMA<br/>DIGITALE E REPOSITORY<br/>SPECIFICA SERVIZIO<br/>016 APPOSIZIONE FIRMA DIGITALE<br/>XADES</b> | GATEFIRE—SER-016<br><br>Pag. 2 di 11 |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|

## 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   | Interfaccia di richiamo (input)                             | 3  |
| 5.1.1 | Metodo firmaXades                                           | 3  |
| 5.2   | Interfaccia di output con Codice esito = 1 (ok)             | 8  |
| 5.2.1 | Metodo firmaXAdES                                           | 8  |
| 5.3   | Interfaccia di output con Codice esito $\neq$ 1 (Nok)       | 9  |
| 5.3.1 | Metodo firmaXades                                           | 9  |
| 5.3.2 | Codici di errore                                            | 10 |
| 5.4   | Tipologie di interfaccia richieste                          | 11 |

|                                                                                   |                                                                                                                                                      |                                                                           |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
|  | <p align="center"><b>GATEFIRE-GATEWAY DI FIRMA<br/>DIGITALE E REPOSITORY<br/>SPECIFICA SERVIZIO<br/>016 APPOSIZIONE FIRMA DIGITALE<br/>XADES</b></p> | <p align="center">GATEFIRE—SER-016</p> <p align="center">Pag. 3 di 11</p> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|

## 1. Obiettivi

### 1.1 Scopo del servizio

Il metodo **firmaXades** 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 XADES, ad un file di tipo xml.

Questi metodi firmano utilizzando la Certification Authority richiesta dall'applicativo chiamante.

Modalità di esecuzione: sincrona.

## 2. Fruitore

Fruitore 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 (**firmaXadesRemota**) o automatica (**firmaXadesAutomatica**)
- delle credenziali della CA dell'utente

### 5.1 Interfaccia di richiamo (input)

#### 5.1.1 Metodo *firmaXades*

Struttura:

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:gat="http://www.csi.it/gatefire/">
  <soapenv:Header/>
  <soapenv:Body>
    <gat:firmaXAdES>
      <attachment>
        <file>cid:1461656719233</file>
        <fileName>ordinativo_non_firmato.xml</fileName>
      </attachment>
      <xadesInput>
        <callInfo>
          <applicationCode>NOME_APPLICAZIONE</applicationCode>
        </callInfo>
      </xadesInput>
    </gat:firmaXAdES>
  </soapenv:Body>
</soapenv:Envelope>
```

|                                                                                   |                                                                                                                                                      |                                                                           |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
|  | <p align="center"><b>GATEFIRE-GATEWAY DI FIRMA<br/>DIGITALE E REPOSITORY<br/>SPECIFICA SERVIZIO<br/>016 APPOSIZIONE FIRMA DIGITALE<br/>XADES</b></p> | <p align="center">GATEFIRE—SER-016</p> <p align="center">Pag. 4 di 11</p> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|

```

    <caCode>INFOCERT</caCode>
    <codiceFiscale>XXXXXXXXXXXXXXXXXX</codiceFiscale>
    <collocazione>010666</collocazione>
  </callInfo>
  <markIdentity>
    <!--Optional:-->
    <password>?</password>
    <!--Optional:-->
    <user>?</user>
  </markIdentity>
  <requiredMark>>false</requiredMark>
  <xpath></xpath>
</xadesInput>
<identity>
  <password>xxxxx</password>
  <user>xxxxxx</user>
  <sessionId></sessionId>
</identity>
</gat:firmaXAdES>
</soapenv:Body>
</soapenv:Envelope>

```

#### Descrizione delle sezioni

- **attachment:** contiene il file da firmare
- **identity** per ARUBA e Infocert
  - *user*
  - *password*
  - *otp*: (in alternativa a *SessionId*) se specificato viene chiamato il servizio per la firma remota, altrimenti quello per la firma automatica
  - *sessionId*: (in alternativa a *otp*)

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
- **xadesInput:**
  - *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, UANATACA o ARUBA)
    - *codiceFiscale*
    - *collocazione* (obbligatorio identificativo ASL chiamante, es per TO5 utilizzare il codice 10205)

|                                                                                   |                                                                                                                                                            |                                                                 |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
|  | <p align="center"> <b>GATEFIRE-GATEWAY DI FIRMA<br/> DIGITALE E REPOSITORY<br/> SPECIFICA SERVIZIO<br/> 016 APPOSIZIONE FIRMA DIGITALE<br/> XADES</b> </p> | <p align="center"> GATEFIRE—SER-016<br/><br/> Pag. 5 di 11 </p> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|

- *dominio* (opzionale. necessario solo se una *collocazione* ha più domini configurati per quel tipo di firma)

|                                                                                   |                                                                                                                                |                                      |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
|  | <b>GATEFIRE-GATEWAY DI FIRMA<br/>DIGITALE E REPOSITORY<br/>SPECIFICA SERVIZIO<br/>016 APPOSIZIONE FIRMA DIGITALE<br/>XADES</b> | GATEFIRE—SER-016<br><br>Pag. 6 di 11 |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|

| Informazione di input              | Riferimento (Entità.attributo)                                                | Obbligatorio                                                                                   | Esempio                                                                                                  |
|------------------------------------|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| file da firmare                    | Sezione <attachment><br><file>?</file><br><fileName>?</fileName>              | Si                                                                                             | <attachment><br><file>cid:123456789012</file><br><fileName>FileDaFirmare.pdf</fileName><br></attachment> |
| otp                                | Sezione <identity><br><otp>?</otp>                                            | No<br>Se presente indica firma digitale REMOTA,<br>Se assente indica firma digitale AUTOMATICA | <otp>1234567890</otp><br>(può essere ricavato utilizzando il servizio a disposizione)                    |
| user_id<br>(delle credenziali CA)  | Sezione <identity><br><user>?</user>                                          | Si                                                                                             | <user>user_remoto</user>                                                                                 |
| password<br>(delle credenziali CA) | Sezione <identity><br><password>?</password>                                  | Si                                                                                             | <password>passw</password>                                                                               |
| Pin                                | Sezione <identity><br><pin>?</ pin >                                          | Si<br>Vale per UANATACA                                                                        | <pin>1234</ pin >                                                                                        |
| codice CA                          | Sezione<br><xadesInput><callInfo><br><caCode>?</caCode>                       | Si<br>Vale ARUBA o<br>INFOCERT o<br>UANATACA                                                   | <caCode>INFOCERT</caCode>                                                                                |
| codice applicazione chiamante      | Sezione<br><xadesInput><callInfo><br><applicationCode>?</applicatio<br>nCode> | Si<br>Deve essere il codice di uno dei verticali configurati                                   | <applicationCode>ESENPAT</a<br>pplicationCode>                                                           |
| codice fiscale utente              | Sezione<br><xadesInput><callInfo><br><codiceFiscale>?</codiceFiscal<br>e>     | Si                                                                                             | <codiceFiscale>BCDFGH70L01<br>D969X</codiceFiscale>                                                      |
| collocazione                       | Sezione<br><xadesInput><callInfo><br><collocazione>?</collocazione<br>>       | Si<br>Deve essere una delle collocazioni configurate                                           | <collocazione>10205</collocazi<br>one>                                                                   |
| dominio                            | Sezione<br><xadesInput><callInfo><br><dominio>?</dominio>                     | No<br>Ricavato dalla configurazione se non specificato                                         |                                                                                                          |
| xpath                              | Sezione <xpath></xpath>                                                       | No<br>L'espressione xpath da                                                                   | <xpath></xpath>                                                                                          |

|                                                                                   |                                                                                                                                |                                      |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
|  | <b>GATEFIRE-GATEWAY DI FIRMA<br/>DIGITALE E REPOSITORY<br/>SPECIFICA SERVIZIO<br/>016 APPOSIZIONE FIRMA DIGITALE<br/>XADES</b> | GATEFIRE—SER-016<br><br>Pag. 7 di 11 |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|

| Informazione di input | Riferimento (Entità.attributo)                              | Obbligatorio                                                                                 | Esempio                             |
|-----------------------|-------------------------------------------------------------|----------------------------------------------------------------------------------------------|-------------------------------------|
|                       |                                                             | utilizzare per identificare il blocco XML da sottoporre al processo di firma XAdES a blocchi |                                     |
| richiesta marcatura   | Sezione <xadesInput><br><requiredMark>>false</requiredMark> | Sì<br>Sempre “false”                                                                         | <requiredMark>>false</requiredMark> |

|                                                                                   |                                                                                                                                                      |                                                                           |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
|  | <p align="center"><b>GATEFIRE-GATEWAY DI FIRMA<br/>DIGITALE E REPOSITORY<br/>SPECIFICA SERVIZIO<br/>016 APPOSIZIONE FIRMA DIGITALE<br/>XADES</b></p> | <p align="center">GATEFIRE—SER-016</p> <p align="center">Pag. 8 di 11</p> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|

**Esempio:**

```

<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:gat="http://www.csi.it/gatefire/">
  <soapenv:Header/>
  <soapenv:Body>
    <gat:firmaXAdES>
      <attachment>
        <file>cid:1461656719233</file>
        <fileName>ordinativo_non_firmato.xml</fileName>
      </attachment>
      <xadesInput>
        <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>
      </xadesInput>
      <identity>
        <password>xxxxx</password>
        <user>xxxxxx</user>
        <sessionId></sessionId>
      </identity>
    </gat:firmaXAdES>
  </soapenv:Body>
</soapenv:Envelope>

```

## 5.2 Interfaccia di output con Codice esito = 1 (ok)

### 5.2.1 Metodo firmaXAdES

Struttura:

```

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

```



|                                                                                   |                                                                                                                                |                                      |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
|  | <b>GATEFIRE-GATEWAY DI FIRMA<br/>DIGITALE E REPOSITORY<br/>SPECIFICA SERVIZIO<br/>016 APPOSIZIONE FIRMA DIGITALE<br/>XADES</b> | GATEFIRE—SER-016<br><br>Pag. 9 di 11 |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|

```

</result>
<attachment>
  <file>?</file>
  <fileName>ordinativo_da_firmare.xml</fileName>
</attachment>
</return>
</ns3:firmaXAdESResponse>
</soap:Body>
</soap:Envelope>

```

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

### 5.3 Interfaccia di output con Codice esito <> 1 (Nok)

#### 5.3.1 Metodo firmaXades

Struttura:

```

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

```

| Informazione di output           | Riferimento (Entità.attributo)                   |
|----------------------------------|--------------------------------------------------|
| codice di errore gatefire        | Sezione <result><br><errorCode>?</errorCode>     |
| descrizione dell'errore gatefire | Sezione <result><br><description>?</description> |

|                                                                                   |                                                                                                                                |                                              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
|  | <b>GATEFIRE-GATEWAY DI FIRMA<br/>DIGITALE E REPOSITORY<br/>SPECIFICA SERVIZIO<br/>016 APPOSIZIONE FIRMA DIGITALE<br/>XADES</b> | <b>GATEFIRE—SER-016</b><br><br>Pag. 10 di 11 |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|

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

### 5.3.2 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 |

|                                                                                   |                                                                                                                                |                                       |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
|  | <b>GATEFIRE-GATEWAY DI FIRMA<br/>DIGITALE E REPOSITORY<br/>SPECIFICA SERVIZIO<br/>016 APPOSIZIONE FIRMA DIGITALE<br/>XADES</b> | GATEFIRE—SER-016<br><br>Pag. 11 di 11 |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|

|          |          |                                                                                                                                 |
|----------|----------|---------------------------------------------------------------------------------------------------------------------------------|
|          | 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                                                                                 |
| Uanataca | 401      | Utente non autorizzato                                                                                                          |
|          | 422      | Request errata                                                                                                                  |

#### 5.4 Tipologie di interfaccia richieste

È previsto l'interfacciamento verso i seguenti sistemi:

- CA Aruba
- CA Infocert
- CA Uanataca