

# **Firma Elettronica Qualificata**

Specifica delle API  
per l'integrazione  
delle applicazioni

**Versione: 3.2b**

**Luglio 2023**


**LAZIOCREA S.P.A.**

SEDE LEGALE E AMMINISTRATIVA: VIA DEL SERAFICO, 107 00142 ROMA –

T +39 06 515631 F +39 06 51563611

UFFICI: VIA ADELAIDE BONO CAIROLI, 68 – ROMA 00145 –

T +39 06 51689800 – F +39 06 51892207


	<b>Firma Digitale Qualificata</b> <b>API per l'integrazione Applicativa</b> Specifica delle API	Rev.	3.2b
		Data	07/2023
		Pag. <b>2</b> a <b>11</b>	

## Sommario

1	Stato del documento .....	3
2	Premessa .....	4
3	API per l'integrazione applicativa.....	6
3.1	Modello di autenticazione.....	6
3.2	API di Firma .....	7
3.2.1	/certificate .....	7
3.2.2	/session.....	8
3.2.3	/session/close.....	8
3.2.4	/otp.....	8
3.2.5	/sign/(st) - con OTP.....	9
3.2.6	/sign/(st) - con sessione.....	9
3.2.7	/sign/(st)/multiple - firma automatica .....	10
3.2.8	/sign/(st)/multiple - firma massiva con sessione .....	10
3.2.9	Transcodifica parametri input .....	11
3.2.10	Richiesta Credenziali OAuth per invocazione API .....	11
3.2.11	Descrizione OpenAPI V3 .....	11

## Indice delle Figure

Figura 1: Modello per l'integrazione di servizi applicativi.....	6
--	---

	<b>Firma Digitale Qualificata</b> <b>API per l'integrazione Applicativa</b> Specifica delle API		Rev.	3.2b
			Data	07/2023
	Pag. <b>3</b> a <b>11</b>			

## 1 Stato del documento


Titolo	Specifiche per l'integrazione applicativa dei servizi di firma digitale		
Versione	3.2b	10/07/2023	
Tipo	Specifica di API		
N. Pagine	11		
Diffusione	<input type="checkbox"/> Riservata	<input type="checkbox"/> Interna	<input checked="" type="checkbox"/> Pubblica
Status	<input type="checkbox"/> In lavorazione	<input type="checkbox"/> Bozza	<input checked="" type="checkbox"/> Pubblicato

### Approvazioni

	Nome e Cognome	Data	Firma
Redatto da	Alessio Gramgni	21/02/2023	
Verificato da	Dante Chirolì	21/02/2023	
Approvato da	Andrea Tomei	21/02/2023	

### Revisione

Ver.	Redatto	Verifica	Approvato
1	Dante Chirolì	Andrea Tomei	Andrea Tomei
2	Dante Chirolì	Andrea Tomei	Andrea Tomei
3	Alessio Gramgni	Dante Chirolì	Andrea Tomei

	<b>Firma Digitale Qualificata</b> <b>API per l'integrazione Applicativa</b> Specifica delle API	Rev.	3.2b
		Data	07/2023
		Pag. <b>4</b> a <b>11</b>	

## 2 Premessa

La possibilità di utilizzare la firma digitale qualificata, a piena valenza legale, è un fattore abilitante per la dematerializzazione del supporto cartaceo e la diffusione di servizi informatici in diversi contesti d'utilizzo.

L'Articolo 24 del Codice dell'Amministrazione Digitale, sin dal 2005, definisce le tipologie e la validità dell'apposizione della firma digitale su documenti informatici, ed è stata inoltre recepito in Italia il regolamento europeo eIDAS che disciplina tre distinte tipologie di firme elettroniche:

- **Firma Elettronica** - dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare
- **Firma Elettronica Avanzata (FEA)** - firma elettronica che soddisfa i seguenti requisiti: è connessa unicamente al firmatario, è idonea a identificare il firmatario, è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo, è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.
- **Firma Elettronica Qualificata (FEQ)** – che in aggiunta a quelle di una firma elettronica avanzata possiede queste caratteristiche: è creata su un dispositivo qualificato per la creazione di una firma elettronica, è basata su un certificato elettronico qualificato, **ha effetto giuridico equivalente a quello di una firma autografa.**


Il processo di firma digitale si fonda sulla disponibilità di un Titolare di due chiavi digitali (numeri binari di almeno 2048 bit):

- una chiave PUBBLICA associata dal Certificatore alla identità del Titolare
- un'altra chiave PRIVATA accessibile dal SOLO TITOLARE previa immissione di un PIN.

Utilizzando le suddette chiavi è possibile, partendo da un documento digitale, generare un nuovo file che, per l'appunto, è il file firmato digitalmente. Tale file, anche riferito come "busta crittografica" è un oggetto digitale che racchiude al suo interno il documento originale, l'impronta digitale dell'originale e la chiave pubblica del titolare.

Tale "busta crittografica" può essere di tre distinte tipologie:

- CADES: con suffisso .p7m contiene file digitale di tipo generico, quali, ad esempio: documenti di testo, fogli elettronici, immagini,
- PAdES: con suffisso .pdf, contiene documenti in formato Adobe pdf,

	<b>Firma Digitale Qualificata</b> <b>API per l'integrazione Applicativa</b> Specifica delle API	Rev.	3.2b
		Data	07/2023
		Pag. 5 a 11	

- XAdES; con suffisso .xml per la sottoscrizione elettronica dei documenti in formato XML (fatture, ...).

LAZIOcrea gestisce una fornitura di servizi di firma digitale qualificata resi da un Trust Provider qualificato che rendono disponibili ai Titolari sia servizi di firma remota sia servizi per l'integrazione di servizi applicativi con i servizi di firma digitale.

Questo documento descrive le interfacce (API) per l'integrazione di servizi applicativi con i servizi di firma digitale.

Si precisa che, nel presente documento si utilizzano i termini chiave "DEVE", "DEVONO", "NON DEVE", "NON DEVONO", "È RICHIESTO", "DOVREBBE", "NON DOVREBBE", "RACCOMANDATO", "NON RACCOMANDATO" devono essere interpretati come descritto in BCP 14 [RFC2119] [RFC8174], e solo quando, appaiono in tutte maiuscole.


Si precisa che questo documento NON descrive le procedure per la richiesta e la distribuzione dei dispositivi di firma digitale, ma unicamente le API per l'integrazione di servizi applicativi con i servizi di firma digitale.

Per l'ottenimento dei dispositivi di firma digitale:

- per l'ambito di produzione si DEVE utilizzare l'apposito servizio disponibile e documentato all'indirizzo: <https://firmad.laziocrea.it>;
- per l'ambito di collaudo si DEVE inviare una mail a [kitfdigitale@laziocrea.it](mailto:kitfdigitale@laziocrea.it) avente oggetto: "Richiesta firma digitale di collaudo" e allegando il file excel (vedi allegato 1) con tutte le informazioni richieste.

Si precisa infine che DEVONO essere rispettate le norme relative all'utilizzo delle distinte tipologie di firma, **FEQ remota** e **FEQ automatica**, con specifico riferimento alle limitazioni d'uso dell'ultima; l'attuale Fornitore usa i prefissi

- RHI..... per le firme FEQ remota
- AHI.... per le firme FEQ automatiche.

	<b>Firma Digitale Qualificata</b> <b>API per l'integrazione Applicativa</b> Specifica delle API	Rev.	3.2b
		Data	07/2023
		Pag. <b>6</b> a <b>11</b>	

### 3 API per l'integrazione applicativa

Sono rese disponibili alcune API semplificate per agevolare l'integrazione di servizi applicativi con i servizi di firma digitale. Più precisamente, e con riferimento alla figura seguente,



Figura 1: Modello per l'integrazione di servizi applicativi

diversi servizi applicativi possono accedere alle API di Firma che s'interpone come un Client generalizzato per l'invocazione dei servizi di firma resi dal Fornitore accreditato.

Con tale disegno si possono garantire sia la disponibilità all'utilizzo applicativo d'interfacce semplificate sia un disaccoppiamento dalla natura proprietaria delle API del Fornitore.

Si riportano di seguito le specifiche per le API di Firma.

#### 3.1 Modello di autenticazione

Le risorse delle API sono protette mediante protocollo OAuth2 con flusso di autorizzazione "Client Credentials" che prevede:


- recupero token di autenticazione mediante POST all'endpoint token
- inserimento dell'header "Authorization: Bearer" nelle chiamate alle risorse dell'API

**Si precisa che è altamente sconsigliato e non sicuro implementare manualmente le chiamate di recupero del token, e accesso alle API.**

Il protocollo OAuth2 è ormai da anni uno standard ed esistono librerie, solide, per ogni tipo di linguaggio di programmazione.

Pr approfondimenti sul protocollo si rimanda alla documentazione presente in rete (<https://oauth.net/2/>)

Discovery Endpoint URL	
Collaudo	<a href="https://qiam.regione.lazio.it/oauth2/oidcdiscovery/.well-known/openid-configuration">https://qiam.regione.lazio.it/oauth2/oidcdiscovery/.well-known/openid-configuration</a>
Produzione	<a href="https://iam.regione.lazio.it/oauth2/oidcdiscovery/.well-known/openid-configuration">https://iam.regione.lazio.it/oauth2/oidcdiscovery/.well-known/openid-configuration</a>

	<b>Firma Digitale Qualificata</b> <b>API per l'integrazione Applicativa</b> Specifica delle API	Rev.	3.2b
		Data	07/2023
		Pag. 7 a 11	

Di seguito viene riportata a **puro titolo esemplificativo** la chiamata per il recupero del token

<b>End-Point</b>	token_endpoint vedi tabella
<b>Method</b>	POST
<b>Header</b>	Authorization: Basic {{base64Encode(<<ClienteKey>>:<<ClientSecret>>)}} Content-Type: application/x-www-form-urlencoded
<b>Body</b>	grant_type = client_credentials
<b>Returns (200)</b>	{ "access_token": "18ad0ff7....." "refresh_token": "e58aa63a-497c-3921-b5e1-8882bc934314" "token_type": "Bearer" "expires_in": "3600" }

## 3.2 API di Firma

Le API di Firma sono esposte su due ambienti distinti, sempre in HTTPS:

API Endpoint URL	
Collaudo	<a href="https://gwapi.laziocrea.it/firmaweb">https://gwapi.laziocrea.it/firmaweb</a>
Produzione	<a href="https://gwapi.servicelazio.it/firmaweb">https://gwapi.servicelazio.it/firmaweb</a>


e rendono disponibili i seguenti metodi:

- /certificate
- /session
- /session/close
- /otp
- /sign/(st) – con OTP o con sessione<sup>1</sup>
- /sign/(st)/multiple – Automatica o massiva (in caso di firma massiva è obbligatorio aprire sessione)

**Nota 1:** possibilità di chiamare più volte l'API all'interno della durata di sessione senza richiedere nuovo OTP di seguito un estratto esemplificativo delle chiamate, **per tutti i dettagli si rimanda al descrittore OpenAPI**

### 3.2.1 /certificate

<b>End-Point</b>	<API EndPoint>/certificate/
<b>Scope</b>	Restituisce il certificato X509 (pem) associato alle credenziali di firma
<b>Method</b>	POST
<b>Header</b>	Authorization: Bearer {{access_token}}
<b>Body</b>	{ username(*) string, password(*) string }
<b>HTTP response</b>	200: File PEM contenente il certificato di firma

	<b>Firma Digitale Qualificata</b> <b>API per l'integrazione Applicativa</b> Specifica delle API	Rev.	3.2b
		Data	07/2023
		Pag. 8 a 11	

### 3.2.2 /session

<b>End-Point</b>	<API EndPoint>/otp/
<b>Scope</b>	A fronte di un OTP restituisce una chiave di sessione, della durata di 3 minuti, con quale è possibile firmare più documenti senza richiedere nuovi OTP.
<b>Method</b>	POST
<b>Header</b>	Authorization: Bearer {{access_token}}
<b>Body</b>	<pre>{   username(*)   string,password(*) string,   dispositivo(*) string,   otp(*) string }</pre>
<b>HTTP response</b>	200: {"key": "bQyFAG67KdH23dJ6.....OT3tJwIb2UnMgH81aA=="}


### 3.2.3 /session/close

<b>End-Point</b>	<API EndPoint>/session/close
<b>Scope</b>	Chiude la sessione OTP in corso
<b>Method</b>	POST
<b>Header</b>	Authorization: Bearer {{access_token}}
<b>Body</b>	<pre>{   username(*)   string,password(*) string,   dispositivo(*) string,   otp(*) string,   session(*) string, }</pre>
<b>HTTP response</b>	200: L'otp sarà inviato verso il dispositivo indicato

### 3.2.4 /otp

<b>End-Point</b>	<API EndPoint>/otp/
<b>Scope</b>	Invio di un OTP sul dispositivo
<b>Method</b>	POST
<b>Header</b>	Authorization: Bearer {{access_token}}
<b>Body</b>	<pre>{   username(*) string,   password(*) string,   dispositivo(*) string, }</pre>
<b>HTTP response</b>	202: L'otp sarà inviato verso il dispositivo indicato




	<b>Firma Digitale Qualificata</b> <b>API per l'integrazione Applicativa</b> Specifica delle API	Rev.	3.2b
		Data	07/2023
		Pag. 9 a 11	

### 3.2.5 /sign/{st} - con OTP

<b>End-Point</b>	<API EndPoint>/sign/{st}
<b>Scope</b>	Esegue la firma di un file e restituisce il file firmato
<b>Method</b>	POST
<b>Header</b>	Authorization: Bearer {{access_token}}
<b>[st]</b>	Valore ammesso uno di: pades, cades, xades
<b>Body</b>	<pre> data(*): {   username(*)   string,password(*) string,   dispositivo(*) string,   otp(*) string,   showSignerImage boolean (default: false) } file(*):file string(\$binary) </pre>
<b>HTTP response</b>	200: Stream segnato

### 3.2.6 /sign/{st} - con sessione

<b>End-Point</b>	<API EndPoint>/sign/{st}
<b>Scope</b>	Esegue la firma di un file e restituisce il file firmato
<b>Method</b>	POST
<b>Header</b>	Authorization: Bearer {{access_token}}
<b>[st]</b>	Valore ammesso uno di: pades, cades, xades
<b>Body</b>	<pre> data(*): {   username(*)   string,password(*) string,   dispositivo(*) string,   otp(*) string,   session(*) string,   showSignerImage boolean (default: false) } file(*):file string(\$binary) </pre>
<b>HTTP response</b>	200: Stream segnato

	<b>Firma Digitale Qualificata</b> <b>API per l'integrazione Applicativa</b> Specifica delle API	Rev.	3.2b
		Data	07/2023
		Pag. 10 a 11	

### 3.2.7 /sign/{st}/multiple - firma automatica


<b>End-Point</b>	<API EndPoint>/sign/{st}/multiple
<b>Scope</b>	Esegue la firma di un insieme di file e restituisce un archivio compresso .zip con il file firmati
<b>Method</b>	POST
<b>Header</b>	Authorization: Bearer {{access_token}}
<b>[st]</b>	Valore ammesso uno di: pades, cades, xades
<b>Body</b>	<pre>data(*): {     username(*)<sup>1</sup> string,     password(*)<sup>1</sup> string,     showSignerImage boolean (default: false) } files(*): array elenco di file string(\$binary)</pre>
<b>HTTP response</b>	200: File ZIP contenente i file firmati in input

**Nota 1:** Tali credenziali vanno richieste adHoc e permettono la firma SENZA necessità di OTP

### 3.2.8 /sign/{st}/multiple - firma massiva con sessione

<b>End-Point</b>	<API EndPoint>/sign/{st}/multiple
<b>Scope</b>	Esegue la firma di un insieme di file e restituisce un archivio compresso .zip con il file firmati
<b>Method</b>	POST
<b>Header</b>	Authorization: Bearer {{access_token}}
<b>[st]</b>	Valore ammesso uno di: pades, cades, xades
<b>Body</b>	<pre>data(*): {     username(*)     string,password(*) string,     dispositivo(*) string,     otp(*)<sup>2</sup> string     session(*) string,     showSignerImage boolean (default: false) } file(*): array elenco di file string(\$binary)</pre>
<b>HTTP response</b>	200: File ZIP contenente i file firmati in input

**Nota 2:** la chiave OTP DEVE essere presente ma il suo valore può essere lasciato vuoto

	<b>Firma Digitale Qualificata</b> <b>API per l'integrazione Applicativa</b> Specifica delle API	Rev.	3.2b
		Data	07/2023
		Pag. <b>11</b> a <b>11</b>	

### 3.2.9 Transcodifica parametri input

L'API prevede l'utilizzo di 4 parametri, obbligatori o meno a seconda della risorsa invocata.

In ogni caso è necessario effettuare una transcodifica tra i nomi dei suddetti parametri e quelli ricevuti come credenziali di accesso da parte del Trust Provider<sup>1</sup>.

Di seguito una tabella esplicativa delle transcodifiche da applicare

Credenziali Ricevuta dal Trust Provider <sup>1</sup>	Parametri invocazione API firmaWEB
<i>username</i>	<b>Non usato</b>
<i>password</i>	<b>Non usato</b>
<i>dispositivo</i>	<i>username</i>
<i>pin</i>	<i>password</i>
<i>ID-Otp</i>	<i>dispositivo</i>
<i>Codice OTP inviato di volta in volta tramite il metodo prescelto</i>	<i>otp</i>

**Nota 1:** L'attuale Trust Provider di Regione Lazio è Namirial – Tale transcodifica potrebbe subire variazione in relazione al cambio del Trust Provider.

### 3.2.10 Richiesta Credenziali OAuth per invocazione API

Per il rilascio delle credenziali OAuth utili all'invocazione dell'API si dovrà inviare una mail a [helpdeskconduzione@laziocrea.it](mailto:helpdeskconduzione@laziocrea.it) con il seguente oggetto

{{Ambiente COLLAUDO o PRODUZIONE}} – {{Progetto}} – Richiesta Credenziali - API FirmaWeb

Es. COLLAUDO - RECUP - Richiesta Credenziali API FirmaWeb

Nel copro della mail dovranno essere specificate le seguenti informazioni:

- Nome Progetto
- Referente con relativi contatti
- Divisione Laziocrea di appartenenza / Nome Ente

Il richiedente riceverà ClientID e ClientSecret per la configurazione del flusso ClientCredential

### 3.2.11 Descrizione OpenAPI V3

Il descrittore yaml delle API per l'integrazione dei servizi di firma può essere recuperato sul Portale Sviluppatori di Laziocrea, al seguente indirizzo

Portale Sviluppatori di Laziocrea	
Collaudo	<a href="https://api-store.laziocrea.it/devportal/apis">https://api-store.laziocrea.it/devportal/apis</a>
Produzione	<a href="https://api-store.servicelazio.it/devportal/apis">https://api-store.servicelazio.it/devportal/apis</a>

potete poi ricercare l'API denominata FirmaWeb e nella sezione Overview -> Gateway Environments cliccare su

