Firma Elettronica Qualificata

Specifica delle API per l'integrazione delle applicazioni

Versione: 3.2

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

Sommario

Indice delle Figure

1 Stato del documento

Titolo	Specifiche per l'integrazione applicativa dei servizi di firma digitale		
Versione	3.2	10/07/2023	
Tipo	Specifica di API		
N. Pagine	11		
Diffusione	☐ Riservata	☐ Interna	☑ Pubblica
Status	☐ In lavorazione	☐ Bozza	☑ Pubblicato

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 soddisfi 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,

- 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 integrazioni.fse@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.

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	https://qiam.regione.lazio.it/oauth2/oidcdiscovery/.well-known/openid-configuration
Produzione	https://iam.regione.lazio.it/oauth2/oidcdiscovery/.well-known/openid-configuration

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

End-Point	token_endpoint vedi tabella
Method	POST
Header	Authorization: Basic {{base64Encode(<<ClienteKey>>:<<ClientSecret>>)}} Content-Type: application/x-www-form-urlencoded
Body	grant_type = client_credentials

Returns (200)	{
	"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	https://gwapi.laziocrea.it/firmaweb
Produzione	https://gwapi.servicelazio.it/firmaweb

e rendono disponibili i seguenti metodi:

/certificate
/session
/session/close
/otp
/sign/(st) – con OTP o con sessione[1]
/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

End-Point	<API EndPoint>/certificate/
Scope	Restituisce il certificato X509 (pem) associato alle credenziali di firma
Method	POST
Header	Authorization: Bearer {{access_token}}

Body	{
	username(*) string,
	password(*) string
	}

HTTP response	200: File PEM contenente il certificato di firma

3.2.2 /session

End-Point	<API EndPoint>/otp/
Scope	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.
Method	POST
Header	Authorization: Bearer {{access_token}}

Body	{
	username(*)
	string,password(*) string,
	dispositivo(*) string,
	otp(*) string
	}

HTTP response	200: {"key": "bQyFAG67KDh23dJ6…….OT3tJwIb2UnMgH8laA=="}

3.2.3 /session/close

End-Point	<API EndPoint>/sessione/close
Scope	Chiude la sessione OTP in corso
Method	POST
Header	Authorization: Bearer {{access_token}}

Body	{
	username(*)
	string,password(*) string,
	dispositivo(*) string,
	otp(*) string,
	session(*) string,
	}

HTTP response	200: L'otp sarà inviato verso il dispositivo indicato

3.2.4 /otp

End-Point	<API EndPoint>/otp/
Scope	Invio di un OTP sul dispositivo
Method	POST
Header	Authorization: Bearer {{access_token}}

Body	{
	username(*) string,
	password(*) string,
	disposoitivo(*) string,
	}

HTTP response	202: L'otp sarà inviato verso il dispositivo indicato

3.2.5 /sign/(st) - con OTP

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

3.2.6 /sign/(st) - con sessione

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

3.2.7 /sign/(st)/multiple - firma automatica

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

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

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[1].

Di seguito una tabella esplicativa delle transcodifiche da applicare

Credenziali Ricevuta dal Trust Provider[1]	Parametri invocazione API firmaWEB
username	***Non usato***
password	***Non usato***
dispositivo	*username*
pin	*password*
ID-Otp	*dispositivo*
Codice OTP inviato di volta in volta tramite il metodo prescelto	*otp*

Nota 1: L'attuale Trust Provider di Regione Lazio è Namirial – Tale trascodifica 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 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	https://api-store.laziocrea.it/devportal/apis
Produzione	https://api-store.servicelazio.it/devportal/apis

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