Redattore	*Pasquale Cavone*	*Data creazione 19/05/2025*
Cliente	*Interno*	*Data modifica 19/05/2025*
Documento	*Web Service Firma*	*Versione 1.0*
Revisore	*Leonardo Scardamaglio*	

Sommario

1 Versione documento

Versione	Data	Descrizione
1.0	18/03/2025	-Prima emissione. -Rotta v1. -Metodi sign/xades, sign/cades e sign/pades

2 Introduzione

⚠IMPORTANTE: Prima di usare le chiamate del Web Service contattare l'assistenza per la corretta configurazione dell'ambiente.

Il servizio Web Service Firma espone un'interfaccia per la firma di documenti nei tipi di firma XAdEs, CAdEs e PAdEs. Tutti i tipi di firma con o senza otp e con o senza marca temporale.

La dimensione massima di upload del documento è 125 MB.
La lunghezza massima del nome file di upload è 250 caratteri.
Il file firmato restituito avrà lo stesso nome dell'originale ma con inizio "sign-". Nel caso di firma CAdEs sarà anche aggiunta estensione ".p7m" alla fine.

Chiamate esposte:

- xades: firma XAdEs per la firma di XML.
- cades: firma CAdEs per la firma di documento di formato generico.
- pades: firma PAdEs per la firma di PDF.

Autenticazione delle chiamate: le chiamate dovranno essere autenticate secondo lo standard OAuth attraverso la richiesta di un Token JWT e il suo inserimento come header Bearer token in tutte le chiamate.

Definizione delle costanti:

Il <baseUrl> varia a seconda degli ambienti:
VarHub NG produzione (Empoli) = https://servizi.varhub.it/signature
Ditech produzione (Bologna) = https://servizi.intermediario.ditechonline.it/signature

Il <authBaseUrl> varia a seconda degli ambienti:
VarHub NG produzione (Empoli) = https://isentry.varhub.it
Ditech produzione (Bologna) = https://isentry.intermediario.ditechonline.it

<route> = v1

3 Autenticazione

Servizio web da chiamare	<authBaseUrl>/api/Token/AccessToken
Http Method	POST
Headers	Content-Type: application/json Accept: application/json
Response Status	Status Code: 200 - OK Status Code: 401 - Unauthorized

Payload Request	{
	"apiName": "openBusiness.scope.serviziweb.api",
	"clientName": "openBusiness.client.serviziweb.api",
	"clientSecret": "uKNtPmq49yjLkaYv",
	"password": "<password>",
	"username": "<username>"
	}

Payload Response	In caso di 200: “<token>”
Note	<username>: username assegnata al cliente. <password>: password assegnata al cliente. <token>: token JWT encoded in base64. Il payload di risposta è una stringa che inizia e termina con il carattere apici doppio (“) in cui è racchiuso il token vero e proprio.

4 Firma XAdEs

Servizio web da chiamare	<baseUrl>/api/<route>/sign/xades
Http Method	POST
Headers	Authorization: Bearer <token> Content-Type: multipart/form-data Accept: application/json
Response Status	Status Code: 200 - OK Status Code: 400 - Bad Request Status Code: 401 - Unauthorized Status Code: 403 - Forbidden: coppia username token e username payload non abilitata alla firma.
Payload Request	username=<username> password=<password> withOtp=<withOtp> idOtp=<idOtp> otp=<otp> withTimestamp=<withTimestamp> timestampUsername=<timestampUsername> timestampPassword=<timestampPassword> file=<file>

Payload Response	In caso di 200 viene restuituito un file binario firmato con content type application/octet-stream.
	
	In caso di 400:
	{
	“message”: <errore>
	}

Note	<username>: (string) obbligatorio. Il riferimento alla chiave. Coincide con il numero di dispositivo virtuale assegnato all’utente. <password>: (string) obbligatorio. Il primo fattore di autenticazione per lo sblocco delle operazioni di firma.

	<withOtp>: (boolean) obbligatorio. True se necessario aggiungere codice OTP. <idOtp>: (int) obbligatorio se withOtp=true. L'identificativo del dispositivo OTP necessario per la validazione del codice OTP; se impostato a -1 verrà selezionato automaticamente il primo dispositivo OTP assegnato all'utente in questione. <otp>: (string) obbligatorio se withOtp=true. Il codice OTP utilizzato come secondo fattore di autenticazione nel caso della firma remota. <withTimestamp>: (boolean) obbligatorio. True se si richiede la marcatura temporale associata alla firma del documento. <timestampUsername>: (string) obbligatorio se withTimestamp=true. Username per l'accesso al servizio di marcatura temporale. <timestampPassword>: (string) obbligatorio se withTimestamp=true. Password per l'accesso al servizio di marcatura temporale. <file>: binary format Content-Type: application/octet-stream <errore> stringa esplicativa dell'errore generato dalla richiesta.

5 Firma CAdEs

Servizio web da chiamare	<baseUrl>/api/<route>/sign/cades
Http Method	POST
Headers	Authorization: Bearer <token> Content-Type: multipart/form-data Accept: application/json
Response Status	Status Code: 200 - OK Status Code: 400 - Bad Request Status Code: 401 - Unauthorized Status Code: 403 - Forbidden: coppia username token e username payload non abilitata alla firma.
Payload Request	username=<username> password=<password> withOtp=<withOtp> idOtp=<idOtp> otp=<otp> withTimestamp=<withTimestamp> timestampUsername=<timestampUsername> timestampPassword=<timestampPassword> file=<file>

Payload Response	In caso di 200 viene restuituito un file binario firmato con content type application/octet-stream.
	
	In caso di 400:
	{
	“message”: <errore>
	}

Note	<username>: (string) obbligatorio. Il riferimento alla chiave. Coincide con il numero di dispositivo virtuale assegnato all’utente. <password>: (string) obbligatorio. Il primo fattore di autenticazione per lo sblocco delle operazioni di firma.

	<withOtp>: (boolean) obbligatorio. True se necessario aggiungere codice OTP. <idOtp>: (int) obbligatorio se withOtp=true. L'identificativo del dispositivo OTP necessario per la validazione del codice OTP; se impostato a -1 verrà selezionato automaticamente il primo dispositivo OTP assegnato all'utente in questione. <otp>: (string) obbligatorio se withOtp=true. Il codice OTP utilizzato come secondo fattore di autenticazione nel caso della firma remota. <withTimestamp>: (boolean) obbligatorio. True se si richiede la marcatura temporale associata alla firma del documento. <timestampUsername>: (string) obbligatorio se withTimestamp=true. Username per l'accesso al servizio di marcatura temporale. <timestampPassword>: (string) obbligatorio se withTimestamp=true. Password per l'accesso al servizio di marcatura temporale. <file>: binary format Content-Type: application/octet-stream <errore> stringa esplicativa dell'errore generato dalla richiesta.

6 Firma PAdEs

Servizio web da chiamare	<baseUrl>/api/<route>/sign/pades
Http Method	POST
Headers	Authorization: Bearer <token> Content-Type: multipart/form-data Accept: application/json
Response Status	Status Code: 200 - OK Status Code: 400 - Bad Request Status Code: 401 - Unauthorized Status Code: 403 - Forbidden: coppia username token e username payload non abilitata alla firma.
Payload Request	username=<username> password=<password> withOtp=<withOtp> idOtp=<idOtp> otp=<otp> withTimestamp=<withTimestamp> timestampUsername=<timestampUsername> timestampPassword=<timestampPassword> page=<page> withSignatureField=<withSignatureField> signerImageX=<signerImageX> signerImageY=<signerImageY> signerImageWidth=<signerImageWidth> signerImageHeight=<signerImageHeight> signerImageFontName=<signerImageFontName> signerImageFontSize=<signerImageFontSize> signerImageTextVisible=<signerImageTextVisible> signerImageFieldName=<signerImageFieldName> signerImageImageVisible=<signerImageImageVisible> signerImageImage=<signerImageImage>

	file=<file>

Payload Response	In caso di 200 viene restuituito un file binario firmato con content type application/octet-stream.
	
	In caso di 400:
	{
	“message”: <errore>
	}

Note	<username>: (string) obbligatorio. Il riferimento alla chiave. Coincide con il numero di dispositivo virtuale assegnato all’utente. <password>: (string) obbligatorio. Il primo fattore di autenticazione per lo sblocco delle operazioni di firma. <withOtp>: (boolean) obbligatorio. True se necessario aggiungere codice OTP. <idOtp>: (int) obbligatorio se withOtp=true. L'identificativo del dispositivo OTP necessario per la validazione del codice OTP; se impostato a -1 verrà selezionato automaticamente il primo dispositivo OTP assegnato all'utente in questione. <otp>: (string) obbligatorio se withOtp=true. Il codice OTP utilizzato come secondo fattore di autenticazione nel caso della firma remota. <withTimestamp>: (boolean) obbligatorio. True se si richiede la marcatura temporale associata alla firma del documento. <timestampUsername>: (string) obbligatorio se withTimestamp=true. Username per l’accesso al servizio di marcatura temporale. <timestampPassword>: (string) obbligatorio se withTimestamp=true. Password per l’accesso al servizio di marcatura temporale. <page>: (integer) obbligatorio se withSignatureField=false. Pagina su cui far apparire il riquadro di firma. Per indicare l’ultima pagina pui usare -1. Maggiore o uguale a 1 o uguale a -1.

	<withSignatureField>: (boolean) obbligatorio. True se si desidera applicare la firma sul campo firma digitale nel PDF. <signerImageX>: (integer) obbligatorio se withSignatureField=false. Coordinata orizzontale in pixel su cui posizionare il riquadro di firma, a partire dall'angolo in basso a sinistra della pagina. <signerImageY>: (integer) obbligatorio se withSignatureField=false. Coordinata verticale in pixel su cui posizionare il riquadro di firma, a partire dall'angolo in basso a sinistra della pagina. <signerImageWidth>: (integer) obbligatorio se withSignatureField=false. Larghezza in pixel del riquadro di firma. <signerImageHeight>: (integer) obbligatorio se withSignatureField=false. Altezza in pixel del riquadro di firma. <signerImageFontName>: (int) obbligatorio. Tipo di font utilizzato nel campo testo. Vedi paragrafo Descrizione tipo font name. Valore suggerito 1. <signerImageFontSize>: (integer) obbligatorio. Dimensione del font utilizzato nel campo testo. Valore suggerito 8. <signerImageTextVisible>: (boolean) obbligatorio. True se si desidera visualizzare la parte testuale. <signerImageFieldName>: (string) obbligatorio se withSignatureField=true. Nome del campo a cui applicare la firma. Questo campo deve essere già presente nel file PDF prima di applicare la firma. <signerImageImageVisible>: (boolean) obbligatorio. True se si desidera visualizzare immagine di sfondo al riquadro di firma. <signerImageImage>: (byte[]) facoltativo. Immagine di sfondo al riquadro di firma. Se non valorizzato e signerImageImageVisible=true allora sarà usata l'immagine seguente con dimensione 110x110 pixels

	 <file>: binary format Content-Type: application/octet-stream <errore> stringa esplicativa dell'errore generato dalla richiesta.

7 Descrizione tipo font name

Valore	Descrizione
1	Times-Roman
2	Times-Bold
3	Times-Italic
4	Times-BoldItalic
5	Helvetica
6	Helvetica-Bold
7	Helvetica-Oblique
8	Helvetica-BoldOblique
9	Courier
10	Courier-Bold
11	Courier-Oblique
12	Courier-BoldOblique
13	Symbol
14	ZapfDingbats