

EASYPROCESS

Manuale Utenti

INFORMAZIONI SUL DOCUMENTO

Prodotto	Easyprocess
Classificazione	Normale
Autorizzati	Responsabile di settore; Sviluppatori; Operatori di settore; Terze parti
Versione template	1.0
Versione Documento	1.1
Data creazione	23/06/2023
Data ultimo aggiornamento	28/09/2023
Redatto da	Simona Grandi
Riesaminato da	Simona Nucci
Approvato da	Angelo Russo

STATO DELLE REVISIONI

Data	Versione	Motivo della revisione	Autore
23/06/2023	1.0	Prima redazione	<i>Simona Grandi</i>
28/09/2023	1.1	Revisione Nuove Funzionalità	<i>Simona Grandi</i>

SOMMARIO

INFORMAZIONI SUL DOCUMENTO.....	2
STATO DELLE REVISIONI	2
SOMMARIO	3
SCOPO DEL DOCUMENTO	4
VALIDITÀ	4
2 AVVIO DELL'INCONTRO (ACCESSO COME PARTE INVITATA)	4
2.1 VIDEOCALL	4
2.2 DOWNLOAD	4
2.3 FIRMA	5
2.3.1 FIRMA ONESHOT	5
2.3.2 FIRMA CON TOKEN	8
2.4 ESCI	10
2.5 MANUALE UTENTE	10
3 REQUISITI OBBLIGATORI FIRMA TOKEN	10
3.1 CONFIGURAZIONE PER POSTAZIONI WINDOWS FIRMA TOKEN	10
3.1.1 REQUISITI DI SISTEMA	10
3.1.2 DISPOSITIVI SUPPORTATI	12
3.1.3 COMPONENTI SOFTWARE DA INSTALLARE	12
4 ESECUZIONE DELLA FIRMA.....	13
4.1 SESSIONE DI FIRMA SENZA APPLLET JAVA.....	13
5 F.A.Q.....	16

SCOPO DEL DOCUMENTO

Lo scopo del documento è di guidare gli utenti all'utilizzo della piattaforma per le mediazioni telematiche

VALIDITÀ

Il seguente documento è da ritenersi valido fino alla registrazione di versione successiva che dichiari esplicitamente NON valido l'attuale versione. Il presente documento, in assenza di informazioni specifiche per la versione, è da ritenersi valido per tutte le versioni dell'applicativo.

2 AVVIO DELL'INCONTRO (ACCESSO COME PARTE INVITATA)

Per l'avvio dell'incontro è necessario cliccare sul link che arriva tramite mail ai partecipanti e che le riporta alla schermata di accesso.
 Dopo aver eseguito l'accesso si deve autorizzare il portale all'utilizzo della videocamera e del microfono; una volta concesse le predette autorizzazioni sarà possibile partecipare all'incontro (si precisa peraltro che l'accesso effettivo alla stanza virtuale sarà possibile solo se il mediatore avrà attivato la sessione).

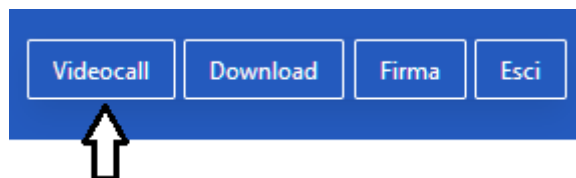
La parte vedrà visualizzate seguenti opzioni



- Videocall
- Download
- Firma
- Esci
- Manuale Utente

2.1 VIDEOCALL

Per partecipare effettivamente all'incontro è necessario cliccare su videocall



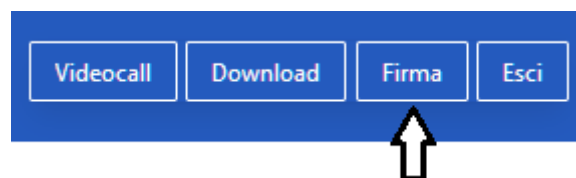
2.2 DOWNLOAD

La sezione download permette di scaricare un documento caricato da parte del mediatore. L'operazione dovrà essere effettuata nel rispetto delle previsioni dei regolamenti degli Organismi e seguendo le indicazioni che saranno fornite dai mediatori.



2.3 FIRMA

La firma digitale potrà essere apposta in due modalità: Oneshot e Token



2.3.1 FIRMA ONESHOT

Il processo di firma OneShot si avvia cliccando sulla voce "Firma" in alto a sinistra e dopo aver inserito i dati riportati come da figura sottostante.

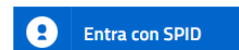
Dati Firmatario: ✕		
Nome e Cognome: Ada	Codice fiscale: LVLD	Num. telefono: 33
Tipo Documento: Scegli tipo documento ▼	Numero Documento <input type="text"/>	
Rilasciato da <input type="text"/>	Data scadenza gg/mm/aaaa <input type="text"/>	
<input type="button" value="Procedi"/>		

Dopo aver inserito i dati e cliccato su "Procedi", cliccare su "Proseguì".

E' necessario aprire il modulo di richiesta e accettarlo, inserire il flag alle voci sottostanti per l'accettazione su Aruba del certificato di firma e cliccare su "Proseguì".

Per autenticarsi bisogna accedere con Spid.

Accedi con SPID



📘 Cliccando sul pulsante *Entra con SPID* ed effettuando l'autenticazione tramite le credenziali della tua identità SPID *Autenticazione*

[Indietro](#)

SPID è il sistema di accesso che consente di utilizzare, con un'identità digitale unica, i servizi online della Pubblica Amministrazione e dei privati accreditati. Se sei già in possesso di un'identità digitale, accedi con le credenziali del tuo gestore. Se non hai ancora un'identità digitale SPID, richiedila ad uno dei gestori.

[Maggiori informazioni su SPID](#)

[Non hai SPID?](#)



Eseguito l'accesso con spid si viene rimandati alla schermata con i dati del firmatario, nella quale deve essere inserito il codice OTP ricevuto sul numero di cellulare, per poi essere convalidato.

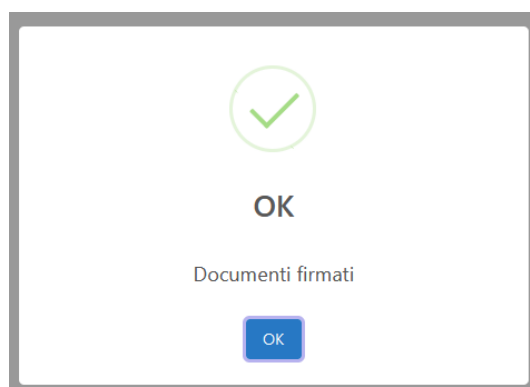
Dati Firmatario: ✕

Nome e Cognome: Ada	Codice fiscale: LVL.D.	Num. telefono: 338
------------------------	---------------------------	-----------------------

Documenti da firmare

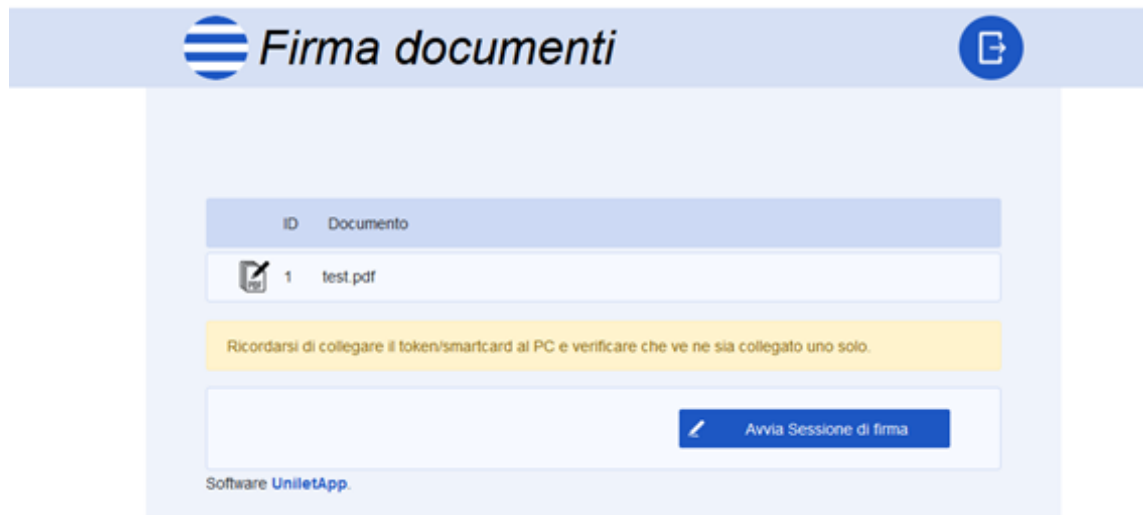
Inviato Codice di controllo al numero di telefono: 338 Invio 1 di 3.

Il seguente messaggio conferma che la firma è avvenuta correttamente.



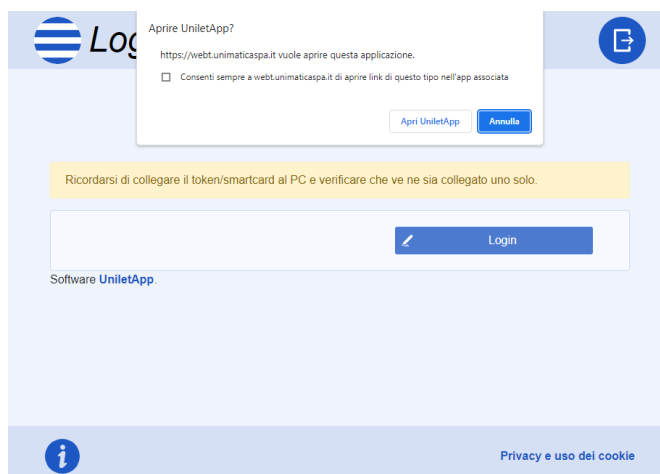
2.3.2 FIRMA CON TOKEN

Per firmare con token è necessario inserire la chiavetta USB per la firma, cliccare sul pulsante Firma e attendere l'apertura dell'elenco dei documenti precedentemente caricati e quindi da dover firmare

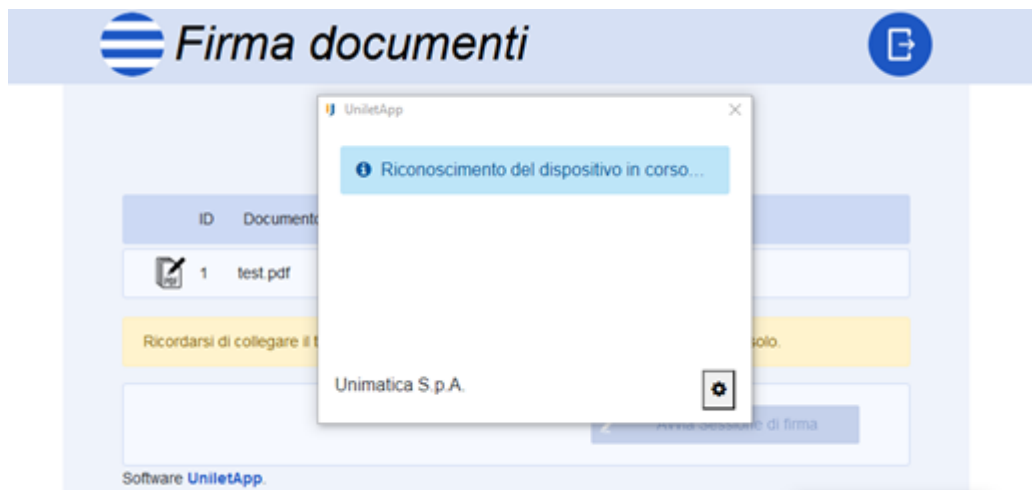


Prima di procedere alla firma deve essere scaricato UniletApp **cfr. capitolo 4 pp. 23**

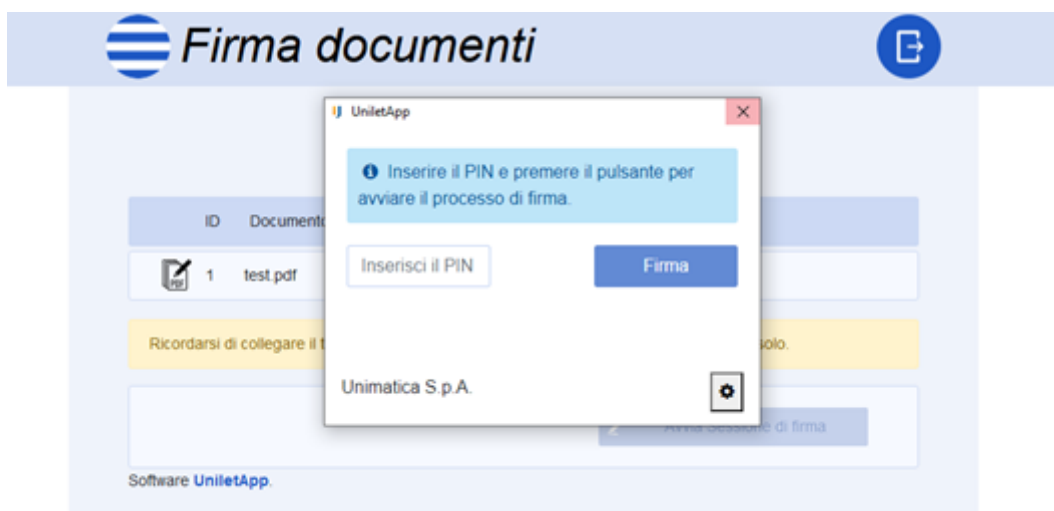
Cliccando poi su "Avvia Sessione di Firma", il portale propone un pop che permette l'apertura di "UniletApp"



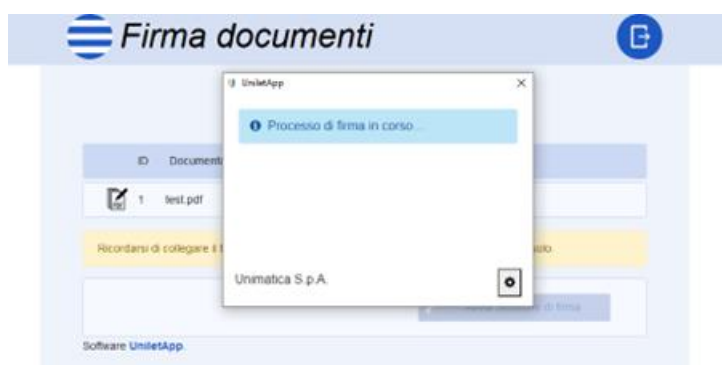
Dopo aver cliccato su "Apri UniletApp" si apre il popup per il riconoscimento del dispositivo usb di firma.



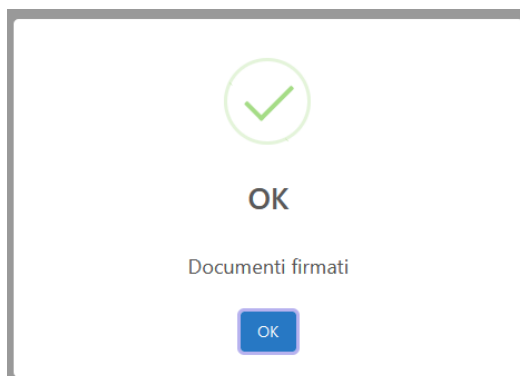
A questo punto viene chiesto di inserire il Pin del certificato di firma.



Inserire il Pin e Cliccare su "Firma".

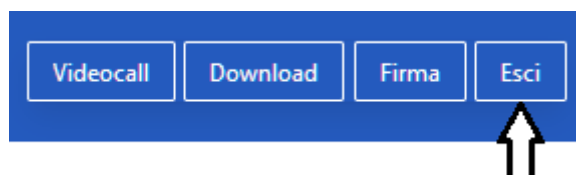


Il portale restituisce l'esito della firma.



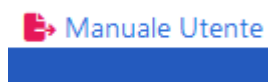
2.4 ESCI

Il pulsante esci permette di uscire dall'incontro per poi accedere successivamente.



2.5 MANUALE UTENTE

Il pulsante Manuale Utente permette di scaricare il Manuale del portale easyprocess.



3 REQUISITI OBBLIGATORI FIRMA TOKEN

3.1 CONFIGURAZIONE PER POSTAZIONI WINDOWS FIRMA TOKEN

La configurazione standard delle postazioni di lavoro per l'uso della soluzione di firma digitale Unimatica prevede:

1 PC Windows con collegamento USB per il dispositivo di firma + 1 monitor + 1 dispositivo di firma (token).

3.1.1 REQUISITI DI SISTEMA

Riportiamo di seguito i prerequisiti per il corretto utilizzo della soluzione di firma digitale tramite Uniserv.

- **RAGGIUNGIBILITÀ DOMINIO UNIMATICA**

Qualora le configurazioni di rete prevedano l'utilizzo di un proxy, esse devono consentire tutte le chiamate in entrata e in uscita (anche quelle non tramite browser) verso il dominio

*.unimaticaspa.it

• SISTEMI OPERATIVI

A partire da Windows >=7 SP1, 32 e 64bit come richiesto da <https://electronjs.org/docs/tutorial/support>

Nota: È opportuno, in alcuni casi necessario, effettuare gli aggiornamenti di Windows segnalati come necessari.

• DIRITTI DI AMMINISTRATORE

Nel caso si effettui l'installazione di UniletApp solo per l'utente corrente non sono necessari i diritti di amministratore. Se si desidera installare UniletApp per tutti gli utenti del PC è necessario effettuare la procedura di installazione con i diritti di amministratore o la presenza di personale tecnico che li possiede.

• REQUISITI HARDWARE

Spazio minimo disponibile su disco rigido: 2.5 GB sufficiente ad installare una JRE aggiornata, i driver del dispositivo di firma e il software di firma e RAM >= 2GB.

• BROWSER

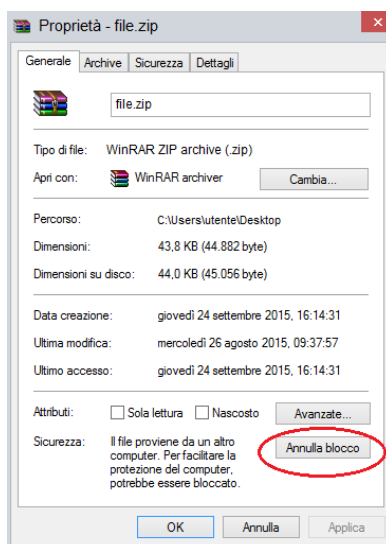
La soluzione di firma UniletApp è compatibile con i browser più utilizzati nelle versioni aggiornate:

- Chrome
- Edge
- Internet Explorer
- Mozilla Firefox

• DOWNLOAD E INSTALLAZIONE DI FILE .ZIP E .EXE

Quando si scaricano dei file .zip o .exe di programmi da Internet, potrebbe succedere che le impostazioni di protezione di Windows, inseriscano automaticamente un blocco.

È necessario rimuovere il blocco ai fini di una corretta installazione delle componenti software richieste.



• DOWNLOAD UNILETAPP

Le risorse di UniletApp da scaricare sono disponibili ai seguenti indirizzi:

Per windows:

<https://web1.unimaticaspa.it/sign-resources/a996d8fc-167a-11ee-be56-0242ac120002/UniletAppSetupJDK.exe>

Per MAC contenete le relative istruzioni per l'installazione:

https://web1.unimaticaspa.it/sign-resources/a996d8fc-167a-11ee-be56-0242ac120002/UniletApp_MacOS_QuickStart.zip

- **INSTALLAZIONE SILENTE FILE .EXE**

Nel caso in cui si deciderà di procedere con una installazione "silente" diversamente da quella standard dell'applicazione sarà necessario eseguire, tramite prompt dei comandi, il seguente comando:

```
UniletAppSetupJDK2.0.2.exe /S > per singolo utente  
UniletAppSetupJDK2.2.2.exe /S /AllUsers > per macchina
```

3.1.2 DISPOSITIVI SUPPORTATI

- **DISPOSITIVI DI FIRMA DIGITALE QUALIFICATA EMESSI TRAMITE UNIMATICA**

- Token usb autoinstallanti (non necessitano di installazione dei driver in locale su client con Windows aggiornato)
- Token usb Athena (necessitano dell'installazione dei driver in locale)

- **DISPOSITIVI DI FIRMA DIGITALE QUALIFICATA EMESSI DA FORNITORE DIVERSO DA UNIMATICA**

Il motore di firma di Unimatica è compatibile con la maggior parte di dispositivi di firma digitale sul mercato, sia che si tratti di smartcard con lettore, di token usb o token con flash memory. Per tutti i dispositivi gestiti vale che, per un corretto funzionamento, è responsabilità dell'utente verificare che sul client siano installati in locale in ambiente Windows i driver aggiornati del dispositivo di firma (ed eventuale lettore) sul quale risiede il certificato di firma digitale qualificata

3.1.3 COMPONENTI SOFTWARE DA INSTALLARE

La predisposizione di una postazione di lavoro per la firma con dispositivo richiede la presenza dei software elencati di seguito. Le componenti vanno installate con diritti di amministratore accettando gli step suggeriti dai wizard e le configurazioni tipo proposte.

- **DISPOSITIVO DI FIRMA**

- **TOKEN USB AUTOINSTALLANTE FORNITO DA UNIMATICA**

Dispositivo hardware senza flash-memory con funzionalità corrispondenti a lettore + smartcard. Su sistema Windows 7 o superiore aggiornati, l'installazione dei driver lettore avviene in automatico quando il dispositivo viene collegato alla postazione, i driver corrispondenti al tipo di card inserito nel dispositivo sono integrati nel motore di firma di Unimatica e per tanto non necessitano di alcuna installazione.

- **TOKEN USB CON O SENZA FLASH-MEMORY DA FORNITORE DIVERSO DA UNIMATICA**

E' necessario installare sul client sotto Windows il pacchetto di driver aggiornato, corrispondente al tipo di card che si intende utilizzare per la firma digitale. I dispositivi con flash memory, con software aggiornato a bordo, in molti casi dispongono di software per l'installazione automatica dei driver in locale o contengono il pacchetto idoneo nella flash-memory del dispositivo. Per individuare il pacchetto e la sua corretta installazione, fare riferimento al fornitore della card.

- **JRE >= 1.8**

E' consigliabile installare e usare la JRE coerente con la versione dei driver del dispositivo di firma in uso.

L'utilizzo di una versione a 64 bit implica che i driver del dispositivo debbano essere a 64 bit (che siano locali o remoti).

NOTA :

Java Runtime Environment, è un ambiente di esecuzione per applicazioni scritte in linguaggio Java.

- **UNILETAPP**

UniletApp è scaricabile seguendo la procedura presente nella pagina di firma.

NOTA :

Le versioni più recenti di UniletApp prevedono l'aggiornamento automatico.

NOTA: la funzione di auto-aggiornamento non funziona in caso di utilizzo di un server proxy

4 ESECUZIONE DELLA FIRMA

Una volta completata la procedura di installazione e configurazione, è opportuno eseguire e portare a termine una sessione di firma.

A tale scopo, è stata messa a disposizione la pagina web di test raggiungibile al seguente link

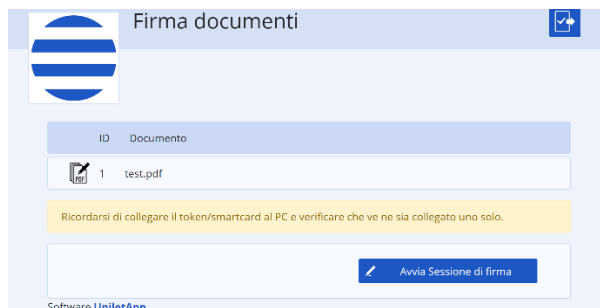
<https://web1.unimaticaspa.it/t-serv/Pages/ConsegnaToken.aspx> che sarà simile alla seguente:



Di seguito viene descritto lo scenario di firma Sessione di Firma senza Applet Java

4.1 SESSIONE DI FIRMA SENZA APPLLET JAVA

In caso di utilizzo della soluzione senza applet si presenterà una schermata simile alla seguente:

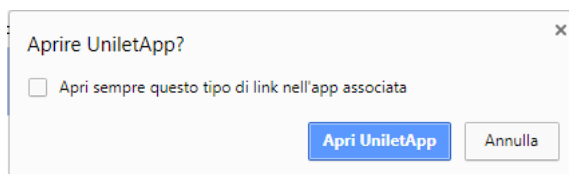


Cliccare su "Avvia sessione di Firma"

Se è la prima volta che si effettua una sessione di firma con UniletApp, potrebbe apparire uno dei seguenti Popup a seconda del browser utilizzato:

Chrome - Internet Explorer - Mozilla Firefox - Microsoft Edge

- CHROME**



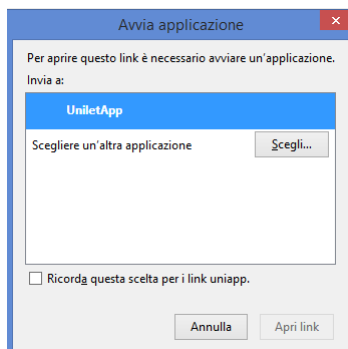
In questo caso si consiglia di mettere il flag su "Apri sempre questo tipo di link nell'app associata" ed in ogni caso cliccare su "Apri UniletApp".

- INTERNET EXPLORER**



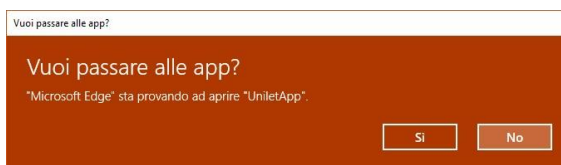
In questo caso si consiglia di togliere il flag dalla voce "Chiedi sempre prima di aprire questo tipo di indirizzo" e successivamente cliccare su "Consenti"

- MOZILLA FIREFOX**

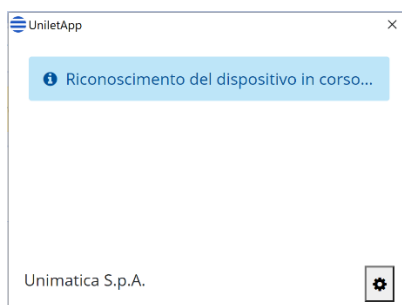


In questo caso occorre selezionare "UniletApp" come mostrato nella precedente figura e si consiglia di impostare il flag della voce "Ricorda questa scelta per i link uniapp" e successivamente cliccare su "Apri link"

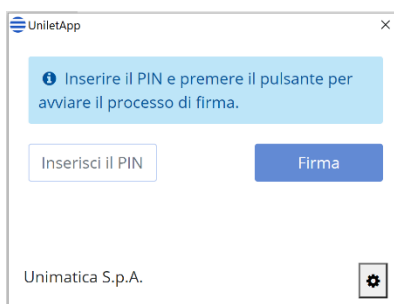
- **MICROSOFT EDGE**



In questo caso occorre cliccare su Sì. A questo punto verrà avviata una finestra di UniletApp, la quale, dopo una fase di inizializzazione, riconosce il dispositivo di firma (token usb o smartcard):

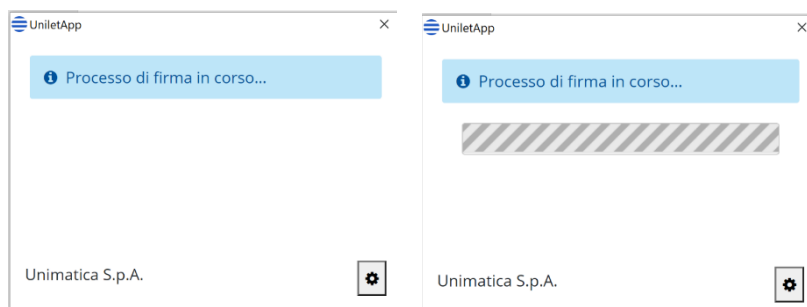


Collegare quindi il dispositivo di firma al pc. Se il dispositivo di firma risulta correttamente rilevato verrà mostrata la richiesta di inserimento pin come mostrato di seguito:

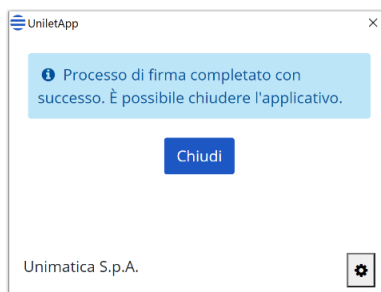


Inserire il PIN e cliccare sul bottone "Firma".

Se il PIN inserito è quello corretto, si avvierà il processo di firma



Se il processo di firma si conclude positivamente si otterrà un risultato simile al seguente: Chiudere il processo cliccando su Chiudi.



Se la sessione di firma si conclude positivamente, verrà mostrata una videata simile alla seguente:



A questo punto il processo di verifica è ultimato e la postazione risulta essere configurata per l'utilizzo del software di firma digitale.

5 F.A.Q.

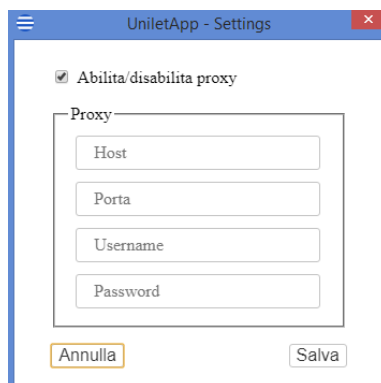
CONFIGURAZIONE PROXY

Nel caso in cui si utilizzi un server proxy per gestire il traffico, è possibile configurarlo nel relativo pannello di UniletApp.

Per configurarlo occorre cliccare sul bottone delle impostazioni come mostrato di seguito:



si aprirà una finestra simile alla seguente:



In questo caso va selezionato il flag "Abilita/disabilita proxy" e vanno inseriti i dati relativi AL proxy utilizzato.
Nel caso il proxy non richieda autenticazione è sufficiente lasciar impostati solo host e porta.

CARD NON RILEVATA

- 1) Verificare che siano stati installati in locale i driver idonei per il dispositivo in uso.
- 2) Se si tratta di un dispositivo tipo token con flash-memory :
 - a. Verificare di aver lanciato l'autorun
 - b. Se il dispositivo è stato lanciato in modalità HID effettuare lo switch alla modalità CCID

NESSUN DRIVER PKCS11 TROVATO

Verificare che siano stati installati in locale i driver idonei per il dispositivo in uso.
Chiedere all'assistenza del fornitore del dispositivo di firma, dov'è possibile recuperare per l'installazione in locale, i driver idonei e aggiornati per l'utilizzo del dispositivo tramite applicativi web ed installarli.

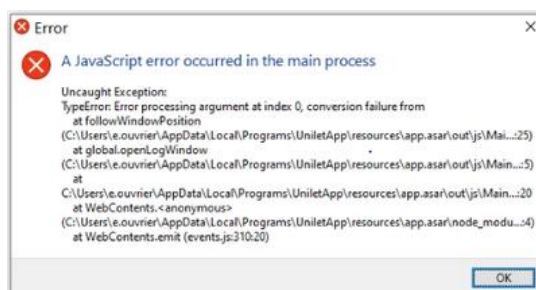
PROBLEMI DI AVVIO UNILETAPP

1. Nel caso in cui si riscontrassero problemi con UniletApp, occorre verificare nei processi attivi, tramite Gestione Attività del sistema operativo, se è presente uno o più processi di "UniletApp.exe". Nel caso fossero presenti occorre terminarli.
2. Nel caso in cui UniletApp non dovesse avviarsi pur essendo installato, si può provare ad effettuare un ripristino delle Impostazioni del browser
3. Nel caso in cui all'avvio di UniletApp dovesse presentarsi un messaggio di errore relativo a java come quello sotto riportato



E' necessario verificare che java sia presente tra le variabili d'ambiente della postazione. Nello specifico occorrerà accedere alla sezione Modifica le Variabili di ambiente del sistema -> variabili d'ambiente e aggiungere la variabile di tipo PATH tra le variabili di sistema con il relativo percorso di java (es. C:\Program Files (x86)\Java\jre1.8.0_311\bin).

4. Nel caso in cui all'avvio di UniletApp dovesse presentarsi un messaggio di errore come quello sotto riportato
 È probabile che la versione di java presente sulla postazione non sia installata correttamente, suggeriamo di disinstallarla ed eseguire una nuova installazione seguita dal riavvio del pc



SECONDA RICHIESTA PIN

Durante una sessione di firma (dopo aver già inserito il PIN) potrebbe venir mostrata una finestra simile alla seguente nella quale viene richiesto nuovamente il PIN:

in questo caso occorre inserire nuovamente il pin e impostare il flag su "ricorda il pin per le firme successive" e cliccare su ok, in questo modo, per le sessioni successive non verrà più richiesto il secondo inserimento del pin.

SBLOCCO PIN

Nel caso in cui dovesse accadere che il PIN venga digitato più volte in modo errato, questo potrebbe bloccarsi (mediamente 3 tentativi).

Per sbloccare il codice PIN è necessario utilizzare il codice PUK fornito insieme al dispositivo di firma che si ha in dotazione.

In caso di utilizzo di dispositivi con Secondary Authentication (doppia richiesta di inserimento PIN) è strettamente necessario utilizzare il software rilasciato dal produttore del dispositivo.

DRIVER

Innanzitutto è necessario individuare se si tratta di un dispositivo USB o di una smart-card. Successivamente verificare chi ha rilasciato il dispositivo, cioè l'ente certificatore CA (Es: Infocert, Aruba, ecc..) questo permette di andare a ricercare e successivamente installare i driver utili direttamente dal sito ufficiale.

Spesse volte i dispositivi di firma hanno a bordo i propri driver che si possono ritrovare all'interno delle cartelle di utility (caso di dispositivi Aruba) o Configurazione/InstallDriver(caso di dispositivi Infocert).

Le stesse informazioni qualora non siano a bordo del dispositivo sono disponibili anche ai seguenti link

Dispositivi rilasciati da Camera di Commercio - **Infocert** :

<https://www.firma.infocert.it/installazione/>

dove scaricare la libreria PKCS11: https://www.firma.infocert.it/software/SafeDive2_setup.zip

Dispositivi **ARUBA**:

<https://www.pec.it/download-software-driver.aspx>

Dispositivi **Poste Italiane**:

<https://postecert.poste.it/firma/download.shtml>

Dal sito <https://www.bit4id.com/> è invece possibile trovare i driver relativi ad alcuni lettori di smart card/token di firma.

Andare nella sezione "Device & Card" e selezionare il modello corrispondente al proprio dispositivo di firma.

Il più comune fra i lettori di smart card utilizzato è il miniLector Evo.

Al seguente link vi sono i driver necessari

https://resources.bit4id.com/#/product/miniLector_EVO selezionare quello del proprio Sistema Operativo (Windows, Linux o macOS).