

I servizi digitali camerali per l'impresa: nuove modalità di accesso ai portali PA e dispositivi di riconoscimento

22 giugno 2021 Sara Pirro, InfoCamere

















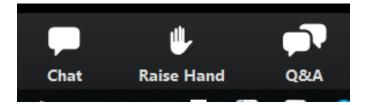






## BENVENUTI AL WEBINAR

I servizi digitali camerali per l'impresa: nuove modalità di accesso ai portali PA e dispositivi di riconoscimento Ora di inizio: 17:00



## Informazioni sullo strumento

**Webcam** e **microfono** sono disabilitati per tutti. È possibile

- scrivere nella chat per problemi tecnici
- fare domande al docente tramite il contenitore Q&A (o D&R),
- alzare la mano per comunicare altre necessità

Lo **streaming audio/video** dipende dalla connessione che si sta utilizzando, se riscontrate problemi si consiglia di controllare la qualità del segnale

# Oggi parleremo di:

- SPID
- CIE
- CNS
- Firma Digitale
- I dispositivi di autenticazione e sottoscrizione delle Camere di Commercio
- La richiesta online

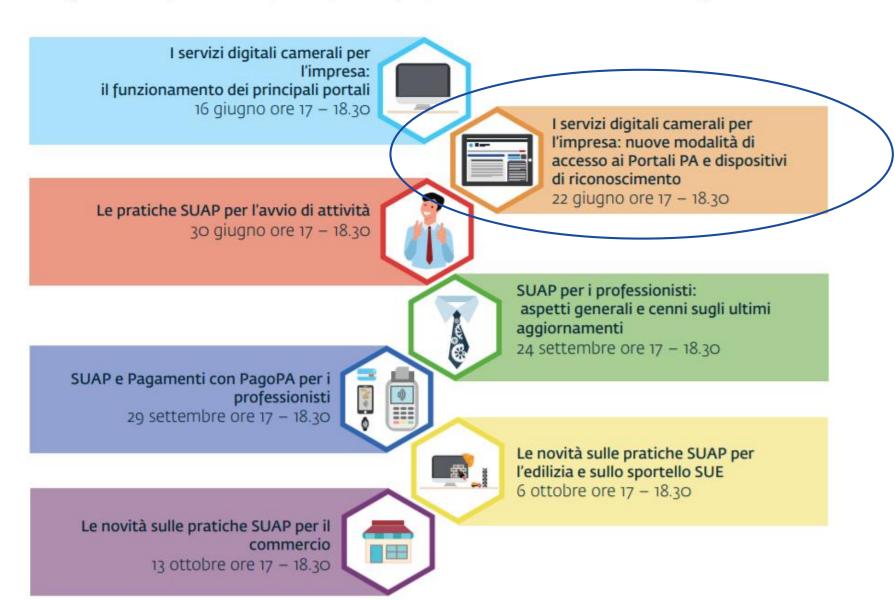
Spazio alle domande





### RIPARTIRE DAL DIGITALE

Programma di formazione per imprese e professionisti sul SUAP e i servizi digitali camerali



Canale YouTube Unioncamere del Veneto con le **registrazioni** degli incontri:

https://youtube.com/playlist?list=PLMnsw r6VbBGQuZ 4vroCqCEDFNeXX pX6

Portale in cui saranno rese disponibili slide e registrazioni di ogni incontro:

http://www.ven.camcom.it/content.asp?ID =1231







## Servizi fiduciari e identificazione elettronica

Un cambiamento culturale importante

Quando si parla di Identità Digitale e di identificazione elettronica è importante il concetto di **fiducia**. Il Regolamento europeo **eIDAS** ci dice che «fiducia» negli ambienti online è:

### Cos'è l'Identità Digitale?

È la rappresentazione virtuale dell'identità reale

Autenticazione informatica: verifica effettuata dal gestore dell'identità digitale, su richiesta del fornitore di servizi, della validità delle credenziali di accesso presentate dall'utente allo stesso gestore, al fine di convalidarne l'identificazione informatica.

Art. 1, lettera f, DPCM 24 ottobre 2014

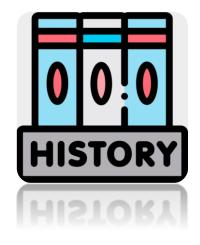
**DELL'UTENTE** PERCEZIONE SUL QUADRO **CERTEZZA GIURIDICO** DEGL SICUREZZA DELL'IDENTITÀ TRASPARENZA CONTROLLO







Breve storia



Se mi si chiede quali sono le cose più importanti da fare, c'è un provvedimento che è la madre di tutti. **Definire un framework per l'autenticazione dell'accesso ai servizi.** Tutti gli amministratori pubblici che vogliono fare servizi online non hanno un modo certificato e uniforme per verificare che chi vuole accedere sia la persona titolata ad accedere. È il punto principale da risolvere.

Giuseppe Stefano Quintarelli, Verso un framework per l'identità digitale, su Agenda Digitale, 13 Marzo 2013

Presidente del Comitato di indirizzo AgID



Sistema Pubblico di Identità Digitale



- È il Sistema Pubblico di Identità Digitale, previsto dalla legge, che permette a cittadini e imprese di accedere con un'unica Identità Digitale ai servizi online di PA e imprese aderenti, tramite la verifica della propria identità.
- È costituito come insieme aperto di soggetti pubblici e privati (qualificati)
- Accesso con SPID da device diversi: computer, smartphone e tablet.
- Il processo di autenticazione informatica è diretto alla verifica dell'identità digitale associata a un soggetto ai fini della erogazione di un servizio fornito in rete.
- Il rilascio e la gestione dell'Identità Digitale SPID può essere effettuato unicamente da Soggetti accreditati ad AgID.



## Normativa SPID

Art. 64 del D. Lgs. 82/05 (CAD) - Sistema pubblico per la gestione delle identità digitali e modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni

Art. 17-ter. Decreto legge 21 giugno 2013, n. 69 (Decreto del Fare) - Sistema pubblico per la gestione dell'identità digitale di cittadini e imprese.

**Decreto Semplificazioni n. 76/2020** convertito in Legge 11 settembre 2020 n. 120



Regolamento UE 2014/910 (eIDAS) – in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno



AGID
AUTORITÀ DI VIGILANZA NAZIONALE

Agenzia per l'Italia Digitale (AgID): Recependo la normativa (CAD e Decreto del FARE) sul dotare ogni cittadino ed impresa di una identità digitale certificata che permetta l'utilizzo in sicurezza dei servizi in rete tramite una identificazione certa, ha predisposto:

- il DPCM 24/10/2014
- la **Determinazione n. 44/2015** (Regolamenti SPID)

AgID inoltre interviene attraverso: Determine, Circolari, Regole tecniche, Avvisi, etc.

STANDARD EU e INTERNAZIONALI

Manuale Operativo IdP: linee guida





Come funziona SPID

Username & Password



**SPID** 

Username e password

OTP by SMS

0

APP mobile

Certificato digitale



Nome utente
OTP

#### LIVELLO 1

Es. accesso alle sezioni informative di un portale pubblico

#### **LIVELLO 2**

INPS, AdE, impresa.italia.it, impresainungiorno, etc.

#### LIVELLO 3

Es. accesso ai portali con dati sensibili (sanitari)





#### Perché ha rilievo l'Identità Digitale

## Dove puoi usare **SPID**?

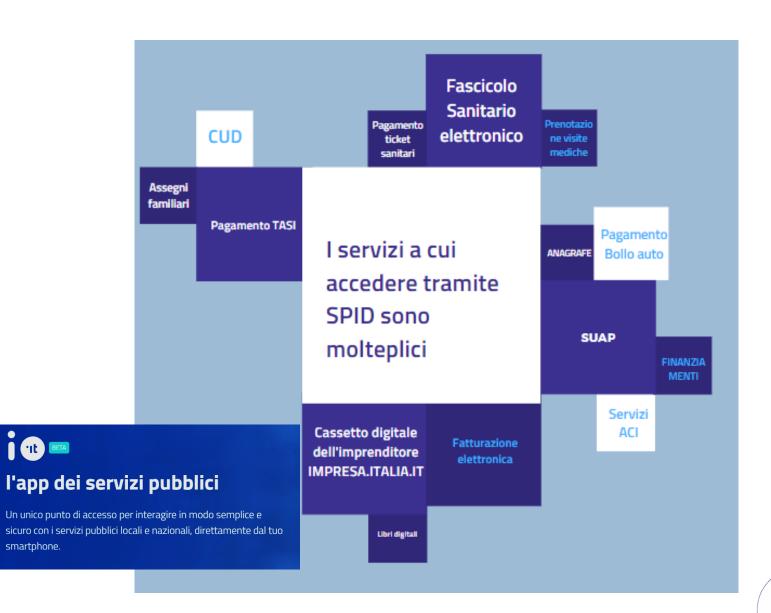
https://www.spid.gov.it/servizi

Avanzamento trasformazione digitale:

https://avanzamentodigitale.italia.it/it/progetto/spid

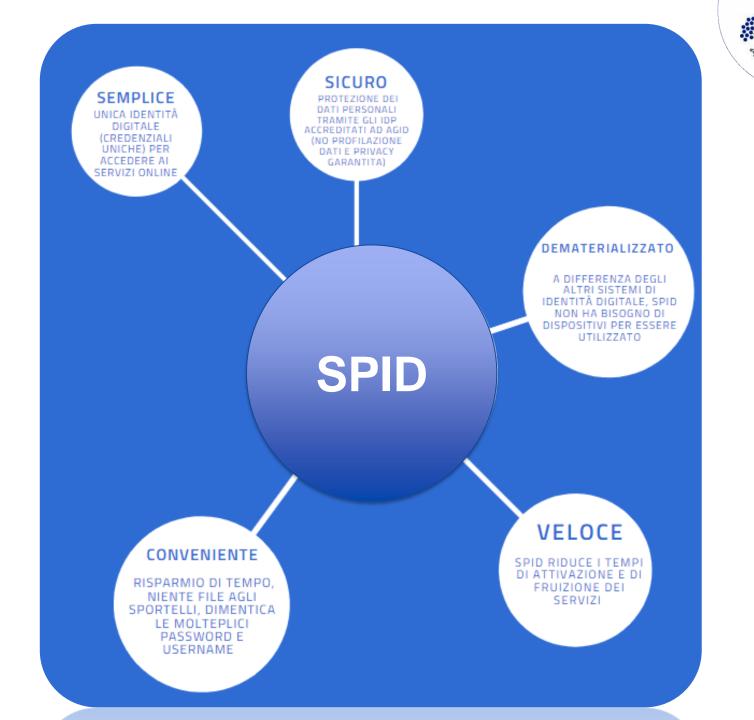
I BETA

smartphone.





"All you need, you already have"





## Nodo elDAS

- Miguel, un cittadino Spagnolo, vuole registrare on line il suo nuovo indirizzo in Italia
- Per verificare l'identità di Miguel, la pubblica amministrazione comunica con il nodo elDAS nazionale
- Il nodo elDAS italiano trasmette la richiesta al nodo elDAS in Spagna
- L'identità di Miguel è verificata dagli Identity Providers spagnoli
- L'identità verificata è inviata all'amministrazione italiana, permettendo a **Miguel di** accedere al servizio online

Il nodo elDAS si basa sull'interoperabilità transfrontaliera delle identità digitali (elD) e la sua implementazione consente:

- ai cittadini italiani di utilizzare le proprie credenziali SPID o CIE per accedere ai servizi pubblici online europei;
- ai cittadini europei di utilizzare i propri schemi di identità nazionale per accedere ai servizi online della Pubblica Amministrazione italiana.



Dove puoi usare il login with eIDAS? https://www.eid.gov.it/servizi









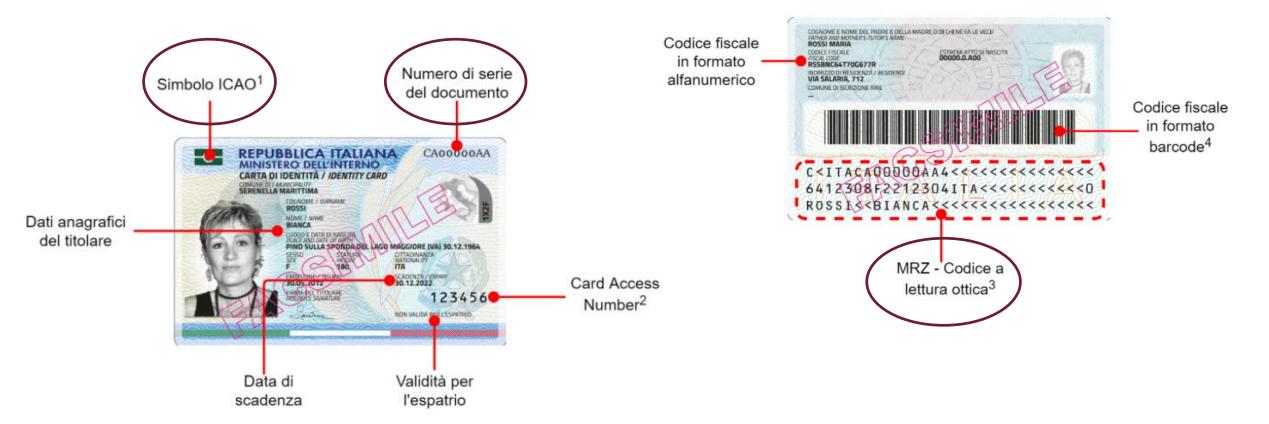
Identità digitale, domicilio digitale e accesso ai servizi digitali, art. 24, DL n. 76/2020

Secondo il **Titolo III** (Misure di semplificazione per il sostegno e la diffusione dell'amministrazione digitale) del Decreto Semplificazioni (decreto legge n. 76/2020 entrato in vigore il 17 luglio 2020 convertito in Legge 120/2020), tutte le amministrazioni locali e centrali, gli enti pubblici e le agenzie, dovranno consentire ai cittadini/imprese di accedere ai propri servizi digitali previa identificazione informatica effettuata esclusivamente attraverso SPID, tramite la Carta d'Identità Elettronica (CIE) e tramite Carta Nazionale dei Servizi (CNS).





## Caratteristiche della CIE: dal 2001 al 2021



Il **microchip contactless** (senza contatto) integrato nel documento rende la CIE uno **strumento** unico e sicuro per la verifica dell'identità del titolare e **per l'accesso** ai servizi online.



### **Autenticazione con CIE**



3 modalità di utilizzo

Entra con CIE consente l'accesso ai servizi online come previsto dall'art. 64 del CAD. La CIE è uno strumento di identità digitale riconosciuto anche in Europa.



## Entra con CIE

- Strumento di verifica dell'identità
- Chiave di accesso ai servizi online
- Fruizione di servizi ad accesso
   veloce (es.: badge identificativi e abbonamenti elettronici)

Consente l'accesso con diverse modalità:

**Desktop** – l'accesso al servizio avviene mediante un computer a cui è collegato un **lettore** di smart card contactless per la lettura della CIE. Per abilitare il funzionamento della CIE sul proprio computer è necessario installare prima il **Software CIE** 

Mobile – l'utente accede al servizio mediante uno **smartphone** dotato di interfaccia NFC e dell'app Cie ID e con lo stesso effettua la lettura della CIE

Desktop con smartphone – l'accesso al servizio avviene da computer e per la lettura della CIE si utilizza lo smartphone dotato di interfaccia NFC e dell'app Cie ID



### Accedi con la CIE in mobilità



https://www.youtube.com/watch?v=yJg9BC2hPt0

CielD è l'app sviluppata dal Poligrafico e Zecca dello Stato Italiano per l'accesso mediante la CIE 3.0.

L'applicazione è disponibile per smartphone con sistema operativo Android 6.0 o superiore, o iOS 13 o superiore, dotati di tecnologia NFC.

#### REGISTRAZIONE CIE SU SMARTPHONE

Aprire l'app e registrare la CIE inserendo il PIN di otto cifre, avvicinare la Carta al dispositivo quando richiesto. La prima parte del PIN viene consegnata dal Comune in occasione della richiesta di rilascio della CIE, la seconda è recapitata insieme alla Carta.

#### **AUTENTICAZIONE AI PORTALI**

- 1. Aprire il browser sullo smartphone Android/iOS
- digitare l'URL del servizio di interesse e cliccare sul pulsante Entra con CIE
- 3. Verrà avviata automaticamente l'app Cie ID, digitare le ultime 4 cifre del PIN o utilizzare l'impronta digitale
- 4. Inserito il PIN, **poggiare la carta sullo smartphone** per avviare il processo di autenticazione e accedere al servizio





## **Certificati Digitali**

Carta Nazionale dei Servizi e Firma Digitale

Tutti i dispositivi (Smart Card e Token) rilasciati presso gli uffici della **Camera di Commercio** contengono **2 tipi** di certificati:



Certificato di Autenticazione - Carta Nazionale dei Servizi - CNS (accesso a servizi online, portali)



Consente l'identificazione certa dell'utente in rete. Il certificato digitale, contenuto all'interno della CNS, è l'equivalente elettronico di un documento d'identità (come il passaporto o la carta d'identità). Viene emesso da un'apposita Autorità di certificazione (Certification Authority - CA)

Certificato di Sottoscrizione - Firma digitale (firma di documenti)



## Certificato di autenticazione CNS

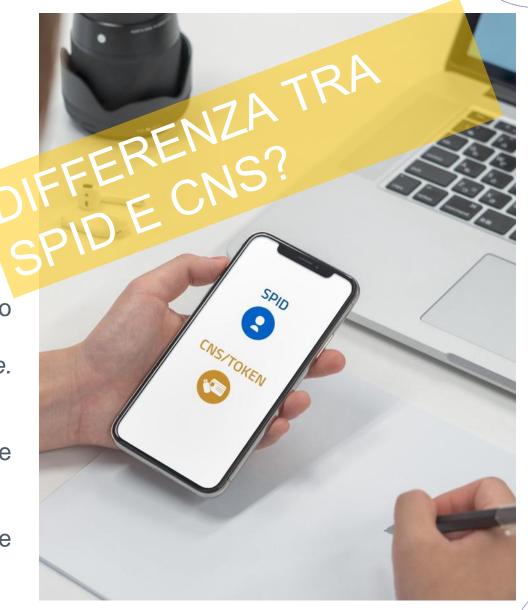
SPID e CNS



**Decreto Semplificazioni** (DL 16 luglio 2020, n. 76 coordinato con la legge di conversione 11 settembre 2020, n. 120) *Misure urgenti per la semplificazione e l'innovazione digitale.* Art. 24: *Identità digitale, domicilio digitale e accesso ai servizi.* 

Gli **unici strumenti** idonei per l'autenticazione ai servizi in rete della PA (INPS, INAIL, AdE) saranno **SPID** e **CIE/CNS**.

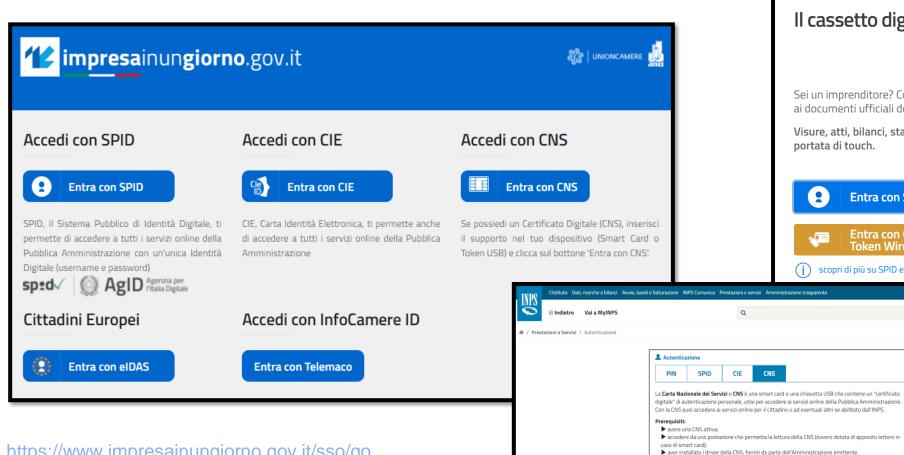
PIN, USERNAME e PASSWORD non verranno più utilizzate e perderanno il requisito di idoneità legale.





Esempi di accesso con CNS, SPID e CIE

Alcuni casi d'uso





Dopo aver verificato i prerequisiti esegui le seguenti operazioni: ▶ inserisci la CNS nel lettore di smart card o norta LISR-

della CNS contiene il tuo codice fiscale tra gli elementi di identificazione:

▶ premi il pulsante PROCEDI, ti verranno elencati tutti i certificati di identificazione personale presenti ▶ seleziona il certificato di autenticazione contenuto nella CNS e premi il pulsante OK. Il certificato

inserisci il codice PIN della CNS, fornito dall'Amministrazione emittente; si tratta in genere di un codice composto da 5-8 cifre. Il PIN ha la funzione di prevenire l'utilizzo della CNS da parte di persone

https://www.impresainungiorno.gov.it/sso/go





## Certificato di sottoscrizione

Tipologie di Firme Elettroniche



Firma Elettronica o Firma Elettronica Semplice (FE)

Electronic Signature (ES)



Firma Elettronica Avanzata (FEA)

Advanced Electronic Signature (AES)



Firma Elettronica Qualificata (FEQ)

Qualified Electronic Signature (QES)





Certificati Digitali

f) Interventi sanzionatori

Regolamento per identificazione, europeo autenticazione e firme elettroniche (eIDAS) **EUROP** Regolamento (UE) n. 910/2014 D.lgs. n. 82/2005 (Codice dell'Amministrazione Digitale - CAD), Sezione II (artt.: 24 – 37) **AUTORITÀ EUROPEA** Commissione europea Corte di Giustizia europea Agenzia per l'Italia **AUTORITÀ NAZIONALE** Digitale (AgID) a) Provvedimenti b) Linee guida STANDARD c) Autorizzazioni generali X.509 (ITU) **LEGAL FRAMEWORK** d) Circolari Unione internazionale delle e) Determine telecomunicazioni



# Tipologie di firma elettronica

	Caratteristiche	Normativa	Valore giuridico	Valore probatorio	Esempi
Firma Elettronica Semplice	Sicurezza, integrità, immodificabilità	art. 26 EIDAS	Consente di attribuire atti e fatti giuridicamente rilevanti a una persona fisica	Liberamente valutabile in giudizio in base alle caratteristiche di sicurezza, immodificabilità e integrità	la firma in una mail
Firma Elettronica Avanzata	Immodificabilità del documento dopo la firma, riconducibilità della firma ad una persona	art. 26 EIDAS art. 56 DPCM 22/02/2013	Soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del codice civile (Fa piena prova fino a querela di falso)	Il soggetto a cui tale firma afferisce può disconoscerla. Sta a chi vuole avvalersi degli effetti giuridici di tale firma dimostrarne la conformità	
Firma Elettronica Qualificata	Come la Avanzata ma effettuata con dispositivo di firma con certificati di sottoscrizione	art. 71 CAD art. 2702 Codice Civile	Ha l'efficacia prevista dall'articolo 2702 come la precedente, previa indentificazione informatica sicura del suo autore attraverso un processo che soddisfa i requisiti AgID	II disconoscimento della firma deve essere dimostrato tramite prova contraria	firma digitale



## Caratteristiche delle firme elettroniche

	firma elettronica	firma elettronica avanzata	firma elettronica qualificata	firma digitale
attestazione della volontà	<b>✓</b>	<b>✓</b>	<b>✓</b>	<b>✓</b>
identificazione del firmatario	X	<b>✓</b>	<b>✓</b>	<b>✓</b>
controllo esclusivo del dispositivo	×	<b>✓</b>	<b>✓</b>	<b>✓</b>
controllo sulle modifiche al doc. firmato	×	<b>✓</b>	<b>✓</b>	<b>✓</b>
certificato qualificato	×	×	<b>✓</b>	<b>✓</b>
dispositivo sicuro	×	X	<b>✓</b>	<b>✓</b>





### Quale certificato di sottoscrizione nei dispositivi delle Camere di Commercio?

La Firma Elettronica Qualificata

I certificati di sottoscrizione presenti all'interno dei dispositivi erogati dalle Camere di Commercio permettono di effettuare una firma elettronica qualificata, con lo stesso valore di una firma autografa.

La firma digitale è un particolare tipo di firma elettronica qualificata che trova la propria disciplina solo e soltanto nell'ordinamento italiano (definita dal CAD - art.1, lettera S).

La firma elettronica qualificata (regolamenta da EIDAS, art.3, n. 12) si basa su "un sistema di chiavi crittografate che consente [...] di rendere manifesta, di verificare la provenienza e l'integrità di un documento informatico o di un insieme di essi".



# La firma elettronica qualificata

EIDAS, articoli 30 e 42



La firma elettronica qualificata (FEQ) è il risultato di una <u>procedura informatica</u>, detta validazione, che garantisce l'autenticità, l'integrità e il non ripudio dei documenti informatici.

Possono dotarsi di FEQ **tutte le persone fisiche**: cittadini, amministratori e dipendenti di società e pubbliche amministrazioni.

Per la generazione della firma elettronica qualificata, sono necessari alcuni requisiti:

- elevati livelli di sicurezza dei dispositivi
- conformità al processo di certificazione prescritto a livello comunitario
- AgID valuta la conformità del sistema e degli strumenti di autenticazione utilizzati dal titolare delle chiavi di firma
- essere in linea con le norme per la valutazione di **sicurezza** dei dispositivi come da decisione della Commissione europea 2016/650
- collegare la data e l'ora ai dati in modo da escludere la possibilità di modifiche non rilevabili dei dati



# Firma Digitale

È un particolare tipo di firma elettronica qualificata basato su un sistema di chiavi crittografiche asimmetriche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico.

La firma digitale è basata sulla crittografia a chiave pubblica asimmetrica e si è ormai affermata come principale strumento in grado, allo stato attuale della tecnologia, di **assicurare l'integrità e la provenienza dei documenti informatici**, e quindi di svolgere per questi la funzione che nei documenti tradizionali è assolta dalla firma autografa.



# Firma Digitale

Ogni soggetto possiede 2 chiavi personali:

- ✓ la pubblica KPub (nota a tutti)
- ✓ la segreta KPriv (nota solo al soggetto)

La chiave pubblica serve per **cifrare** (integrità e riservatezza), La chiave privata per **firmare** (autenticità e non ripudio)

La firma digitale utilizza l'algoritmo RSA (da <u>Ronald Rivest</u>, <u>Adi Shamir</u> e <u>Leonard Adleman</u>) che è il primo sistema di crittografia a chiavi pubbliche ed è anche quello **attualmente più diffuso ed utilizzato**.

Può essere usato sia per cifrare sia per firmare digitalmente documenti. È considerato sicuro se sono usate chiavi abbastanza lunghe (almeno1024 bit)



# Firma Digitale

La PKI (Public Key Infrastructure) è un'infrastruttura di sicurezza costituita da protocolli e servizi, per il supporto di applicazioni basate su crittografia a chiave pubblica. La PKI tramite l'utilizzo dei certificati digitali, consente di soddisfare i seguenti requisiti:

- Autenticazione: garantisce l'identità di un titolare
- Confidenzialità: garantisce che solo il destinatario di un messaggio o di un documento possa leggerne il contenuto
- Integrità: garantisce che l'informazione non sia stata alterata nella trasmissione o nell'archiviazione
- **Non ripudio**: garantisce che i partecipanti ad una transazione non possano negare di averla eseguita, il mittente di un messaggio non può negare di averlo spedito e chi lo riceve non può negare di averlo ricevuto



### Validità e Rinnovo

Certificato di autenticazione e sottoscrizione

I certificati digitali contenuti nei dispositivi rilasciati dalla Camera di Commercio hanno **3 + 3** anni di validità. Nei **90 giorni prima** della scadenza è necessario procedere al loro rinnovo per ulteriori 3 anni. Il rinnovo può essere effettuato **una sola volta**. Una volta che i certificati sono scaduti, non è più possibile rinnovarli e si deve richiedere un **nuovo dispositivo**.



## I formati di Firma Digitale

# **PAdES**

PDF Advancede Electronic Signature

Data Format: PDF (part og CADES)

Applicable data: PDF

Relevant Specification: ETSI TS 103 172 ETSI TS 102 778

managerities DEM

Verificabile con software chw legge PDF (adobe)

# CAdES

CMS Advanced Electronic Signature

Data Format: ASN1 and Ber/Der

Applicable data: text and binary file

Relevant standard: ETSI TS 103 173 ETSI TS 101 733

nomefile.P7M

Verificabile con apposito software

Firma

CADES.p7m

# XAdES

XML Advanced Electronic Signature

- Data Format: XMII

Applicable data: text and binary file XMLdata

> Relevant Standard: ETSI TS 103 171 ETSI TS 101 903

> > Nomefile.XML

Verificabile con visulizzatore XML







### **Smart Card**

Caratteristiche e Differenze

#### **Smart Card**

Ha la forma di una **tessera** tipo bancomat da inserire in un lettore di smart card collegato al PC tramite una porta usb. Per il suo funzionamento occorre **scaricare** un apposito software di firma (Dike GoSign o File Protector). Presente microchip crittografico con 2 certificati. Installazione e aggiornamento driver del lettore periodici.



Per usare il dispositivo è necessario acquistare il lettore separatamente e scaricare un programma di firma sul PC









Caratteristiche e Differenze

#### **Token USB**

Trattasi di una chiavetta USB

autoinstallante per la quale non occorre
scaricare apposito software di firma.

Per l'utilizzo non occorre alcune lettore.
Esistono Business Key contenenti un
solo certificato.



Certificato di autenticazione (Identità Digitale per accedere ai servizi online delle P.A.)

Certificato di sottoscrizione (Firma Digitale con valore di firma autografa)

Programma di firma integrato al dispositivo

Utilizzabile senza lettore dedicato (ma solo via USB)



## DNA digitale dell'impresa in un unico dispositivo wireless

Strategia Mobile First



La velocità con cui l'utilizzo dei servizi mobile si sta diffondendo ha reso necessario nell'ambito della firma digitale trovare **soluzioni smart** e di innovazione tecnologica.

Il nuovo token si contraddistingue per il suo potenziale di integrazione nasce infatti per essere **interfacciabile** con i più moderni dispositivi mobile sul mercato, pur mantenendo la stessa funzionalità e usabilità per personal computer e applicazioni precedentemente utilizzate.



# **DigitalDNA Key**

Strumento per la digitalizzazione e semplificazione delle imprese



- ✓ Indipendenza
- ✓ Semplicità di utilizzo
- / Libertà di movimento
- ✓ L'identità digitale per la tua azienda

Il token innovativo dotato di tecnologia Bluetooth





Strumento per la digitalizzazione e semplificazione delle imprese

- La DigitalDNA Key è un dispositivo di ultima generazione per l'autenticazione e la firma digitale (contiene entrambi i certificati)
- Progettato per rendere l'esperienza utente semplice e intuitiva.
- È la chiave per **portare con se l'identità digitale**, sempre e ovunque con facilità e sicurezza
- La soluzione si compone di un token innovativo accompagnato da un'app correlata (DigitalDNA IC), al primo accesso l'utente viene guidato nella procedura di associazione tra la DigitalDNA Key e il dispositivo mobile.







Strumento per la digitalizzazione e semplificazione delle imprese

- Token evoluti dotati d'interfaccia di comunicazione duale: USB e Bluetooth.
- Possibilità di configurare la propria firma remota.
- Il dispositivo in futuro sarà completato con SPID3



Abilita l'imprenditore ad essere digitale «a valore legale»



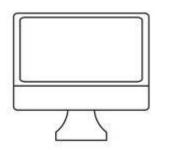
# **Comunicazione duale**

DigitalDNA Key

### Due modalità di utilizzo:

✓ Da desktop in modalità USB tramite il software firma4ng → autoinstallante





✓ Da dispositivi mobili (smartphone o tablet) in modalità Bluetooth tramite

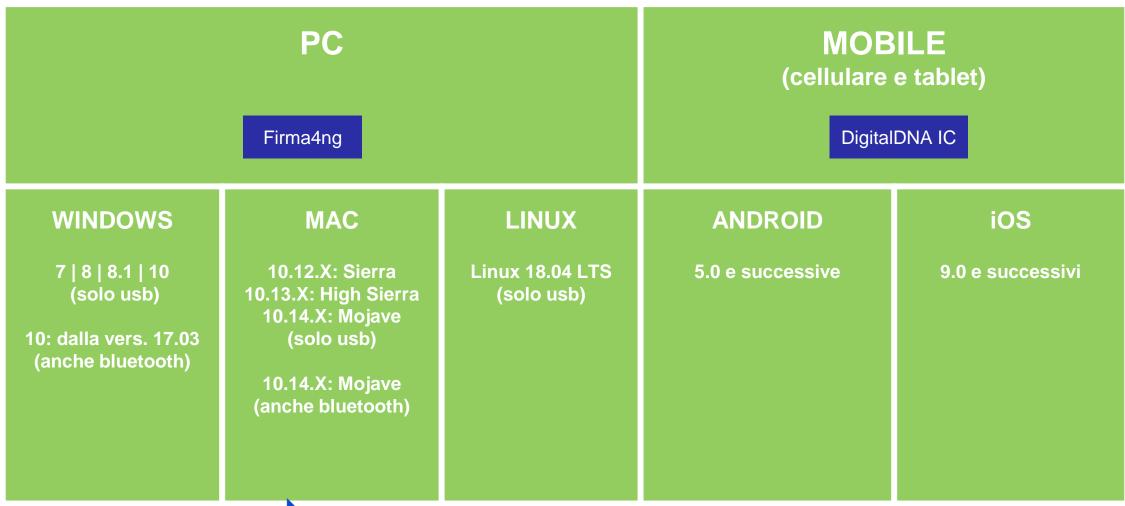
l'apposita app **DigitaIDNA IC** 





# Requisiti di sistema per utilizzo da pc e mobile

DigitalDNA Key









#### INTERRUTTORE DI ALIMENTAZIONE

per attivare o disattivare l'alimentazione del Bluetooth

### **UNICO PULSANTE DI CONTROLLO**

per il controllo di tutte le modalità di funzionamento

**LED**: nei tre colori primari principali

VERDE: modalità USB

BLU: modalità Bluetooth

ROSSO: stato della batteria







La tua impresa sempre in tasca

Così come il token, anche l'App è stata progettata per semplificare al massimo l'esperienza utente e garantire estrema sicurezza nelle operazioni.

Dopo l'abbinamento con il token, si ha libero accesso alle numerose funzionalità dell'app come la **Firma Digitale**, l'**Autenticazione** ai servizi online, la **Verifica** della validità e integrità dei documenti, lo **Storico** dei documenti firmati e delle operazioni effettuate.













# **Pairing**

Associazione dispositivo mobile e DigitalDNA Key





- 2. Attivare il <u>Bluetooth del dispositivo mobile</u> (cellulare o tablet)
- 3. <u>Aprire l'app</u> DigitalDNA IC e assicurarsi che il <u>simbolo del Bluetooth</u> sia di colore blu (acceso)
- 4. <u>Individuare</u> la propria chiavetta con il codice di 6 cifre posto sul retro
- 5. <u>Tenere premuto il pulsante multifunzione</u> della chiavetta fino a quando non chiederà di inserire il PIN (presente nella scratch card virtuale)
- Dopo questi passaggi, la DigitalDNA Key emetterà un <u>suono</u> e l'abbinamento sarà stato eseguito

NB: in caso di malfunzionamento dell'associazione, provare ad attivare la **localizzazione** del cellulare



# App in continuo miglioramento DigitalDNA IC

L'app DigitalDNA Key è in continuo miglioramento e spesso arricchita di nuove funzionalità.

#### Le ultime novità:

- Funzione di **Marcatura temporale**. E' possibile applicare una marca temporale ad un file per accertarne <u>l'effettiva data di creazione</u> e garantirne la <u>validità nel tempo</u>. La funzione si attiva configurando l'app con i dati del proprio Time Stamp Provider (TSA)
- > La funzione di Verifica dei documenti firmati è stata migliorata e semplificata
- Supporto alla nuova versione iOS (versione 13.5)
- > Correzione bug su iOS per la funzione di firma documenti da e-mail
- Miglioramento supporto ad Android 10
- Ottimizzazione consumo della batteria

















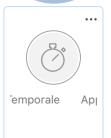
















### Tante funzionalità



L'applicazione è compatibile con i sistemi mobile: **Android 5.x** e successivi e **iOS 9.x** e successivi









# Funzioni dell'App DigitalDNA IC

Non solo la firma, ma molto altro

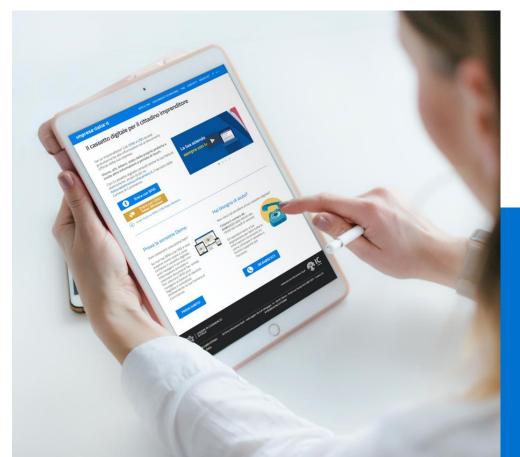
- Firma
- Storico
- Verifica
- Gestione Dispositivo
- FindME
- Ultima posizione rilevata
- Servizi web
- Impostazioni
- Info
- Marca Temporale

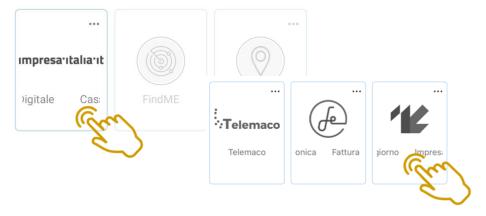
- Cassetto Digitale dell'Imprenditore
- Telemaco
- Fattura Elettronica
- Impresainungiorno
- Diritto annuale
- Atti depositati
- Scuola lavoro
- INPS
- Agenzia delle Entrate
- Agenzia delle Entrate Riscossione



# App DigitalDNA IC: impresa.italia.it e impresainungiorno.gov.it

I widget consentono di accedere direttamente al *cassetto* digitale dell'imprenditore e al portale impresainungiorno





Cliccando sul widget «impresa.italia.it» si apre direttamente il portale attraverso il browser contenuto nell'applicazione: inserendo il PIN (o utilizzando le altre forme di riconoscimento) si accede al *cassetto digitale*.

Quando si accede ad un portale che richiede autenticazione tramite CNS, sia tramite un widget della home sia tramite il browser «servizi web», la DigitalDNA key consente l'accesso tramite bluethooth con l'inserimento del pin (o touch-id o face-id), previo possesso dei requisiti di accesso.



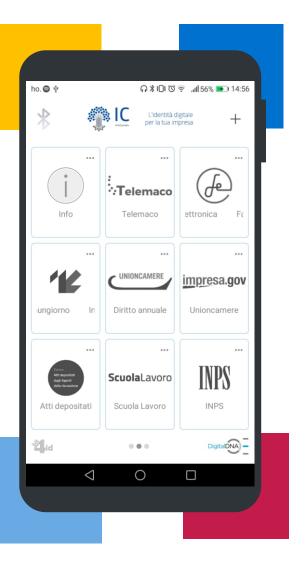
## App DigitalDNA IC: uso come CNS

Accesso ai portali come CNS

Nella seconda pagina dell'applicazione DigitalDNA IC sono salvati come *preferiti* alcuni portali web ai quali è possibile accedere con CNS, secondo le modalità indicate in precedenza.

#### Altresì è possibile:

- utilizzare il widget «Servizi web» come un normale browser, per accedere ai portali web con CNS il browser richiamerà automaticamente la DigitalDNA Key tramite Bluetooth
- salvare ulteriori siti come preferiti.







Caso d'uso









È possibile firmare un documento ricevuto tramite **e-mail**, **WhatsApp** o **Telegram**, senza la necessità di memorizzarlo preventivamente su una cartella locale.

#### Esempio:

- selezionare il file ricevuto su WhatsApp;
- dal menù di sistema scegliere l'applicazione DigitalDNA;
- procedere con la firma del file

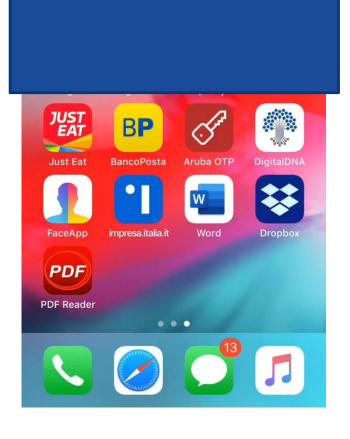




Tante funzionalità

- Come si firma in mobilità
- Come si verifica la firma inserita nel documento
- Come si accede al Cassetto Digitale dell'imprenditore per scaricare la visura e tanti altri documenti sul cellulare/tablet

.... E molto altro





# Utilizzo token DigitalDNA da desktop

InfoCamera

Il software Firma4ng

La prima volta che il token DigitalDNA viene collegato alla porta USB del PC, viene **installata** automaticamente l'applicazione e compare sul desktop la relativa **icona**:



Successivamente è sufficiente cliccare sull'icona per utilizzare i servizi del token DigitalDNA. Ogni volta che si utilizza da PC è necessario che il token sia inserito nella porta USB ma non è necessario accenderlo.



# Firma4ng: avvio software

### Inserire la DigitalDNA Key nella porta USB

### **WINDOWS**

Avviare il programma di installazione (con estensione .exe) con doppio click e seguirne tutti i passi.

Se non si è aperta in automatico, aprire la cartella corrispondente alla DigitalDNA Key da «Esplora Risorse».

#### MAC

Avviare il programma di installazione (con estensione .pkg) e seguirne tutti i passi.

Se non si è aperta in automatico, aprire la cartella corrispondente alla DigitalDNA Key dal Finder.

### LINUX

Estrarre il contenuto dall'archivio individuate dal file con estensione .tar.gz

#### **COME FUNZIONA Firma4ng?**

### Aggiornamento automatico

Il software firma4ng si aggiorna <u>automaticamente</u> ad ogni avvio, qualora siano disponibili nuove versioni e se il computer è <u>connesso ad Internet</u>.



# Tanti vantaggi DigitalDNA Key

- ✓ Possibilità di firmare in mobilità da smartphone/tablet, non è necessario collegare la chiavetta al pc
- ✓ Possibilità di firmare un file contenuto nella e-mail, WhatsApp/Telegram
- ✓ Possibilità di condividere il file firmato tramite WhatsApp/e-mail/Telegram o altra app
- ✓ Tramite l'apposita app, accesso diretto al cassetto digitale dell'imprenditore con possibilità di scaricare/visualizzare la visura e condividerla tramite WhatsApp/e-mail
- ✓ Utilizzo diversificato: utilizzando il pc (Windows, Mac, Linux) tramite il software firma4ng; utilizzando dispositivi mobili (smartphone e tablet) in modalità Bluetooth tramite l'apposita app



## Indirizzi utili: id.infocamere.it

**Digital Identity** è il portale informativo pubblico di InfoCamere per tutte le soluzioni di firma digitale, i servizi legati ad essa, i manuali e la documentazione tecnica.

### Portale Digital Identity:

https://id.infocamere.it/infocamere/home

Guida utente firma4ng e download software:

https://id.infocamere.it/infocamere/download software/download software

Manuale utente app DigitalDNA IC e QR per scaricarla:

https://id.infocamere.it/infocamere/download software/app digital dna

Supporto firma digitale:







# I vantaggi della richiesta online

Il servizio di remotizzazione, avviato in ambito dell'emergenza sanitaria COVID-19, comporta diversi vantaggi:

- 1.Il servizio favorisce lo svolgimento di gran parte delle operazioni per l'ottenimento della CNS/Firma Digitale in remoto
- 2.Il servizio consente all'utente di scegliere, in base alle sue esigenze, la data e ora dell'appuntamento per il riconoscimento
- 3. Se prevista la spedizione, si riceve il dispositivo direttamente a casa o in ufficio



### La richiesta online

Pagina dedicata con informazioni utili sul servizio

https://www.pd.camcom.it/gestisci-impresa/cns-firma-digitale-spid/rilascio-online-firma-digitale



https://www.tb.camcom.gov.it/content/14767/Bisogni/della-Firm/WebID/



https://www.dl.camcom.it/sonoimpresa/sono-impresa-cosa-devo-fare/avere-gli-strumenti-digitali-necessari-sono/firma-digitale-cns/rilascio-online-firma-digitale#div14000060



https://www.vr.camcom.it/it/content/servizi-digitali



https://www.vi.camcom.it/it/servizi/impresa-digitale/firma-digitale-riconoscimento-remoto-viaWebcam.html







Non ho un'indentità/firma digitale (token o smart card)



Tramite operatore con riconoscimento via webcam, se non si è già in possesso di una firma digitale/CNS in corso di validità Ho già un'indentità/firma digitale (token o smart card)



In autonomia con firma digitale attraverso una procedura online per chi avesse già un dispositivo di firma in corso di validità

All riconoscimento può essere fatto con l'operatore tramite piattaforma dedicata





B Il riconoscimento può essere fatto in autonomia dall'utente se già in possesso di CNS in corso di validità e rilasciata dal circuito camerale

La scelta della modalità di riconoscimento avviene prima dell'inizio della compilazione dei dati necessari per la richiesta.



# Documenti accettati per la richiesta online

Con la modalità di identificazione tramite video riconoscimento i documenti di riconoscimento utilizzabili ai fini dell'identificazione sono:

CARTA DI IDENTITÀ
PATENTE DI GUIDA
PASSAPORTO

Il documento di riconoscimento presentato deve essere:

**NON SCADUTO** 

DL 56/2021 (30 SETTEMBRE 2021)

**ORIGINALE** 

**EMESSO DA AUTORITÀ ITALIANA (tranne il passaporto)** 

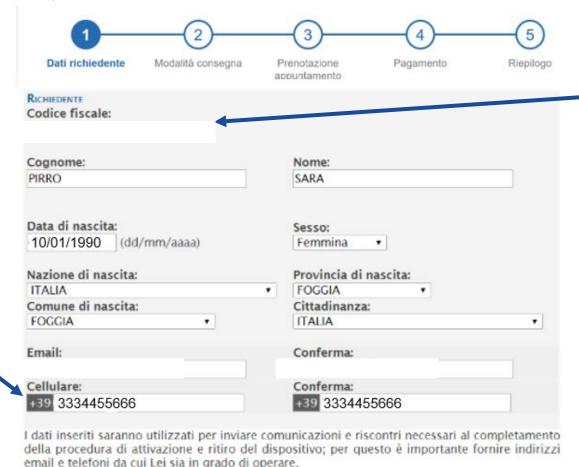


### Emissione dispositivo CNS con identificazione de-visu

Home > Rilascio identità digitale > Emissione dispositivo CNS con identificazione de-visu

Il numero di telefono può essere italiano oppure di un paese della ZONA1\*
(Paesi dello Spazio Economico EU) aderente al Roaming europeo.

Emissione CNS tramite De-visu



Quando si inserisce il Codice Fiscale, viene fatta una verifica sull'anagrafica tributaria della Agenzia delle Entrate e vengono effettuati i controlli incrociati con i campi cognome, nome, data di nascita e sesso.

Univocità indirizzo e-mail e cellulare

\*ZONA1: Austria, Belgio, Bulgaria, Cipro, Croazia, Danimarca, Estonia, Finlandia, Francia - inclusi Guadalupe, Guyana Francese, Martinica, La Reunion, Mayotte -, Germania, Gibilterra, Grecia, Irlanda, Islanda, Lettonia, Liechtenstein, Lituania, Lussemburgo, Malta, **Norvegia**, Olanda, Portogallo, Polonia, Repubblica Ceca, Repubblica Slovacca, **Regno Unito** - inclusi Guernesy, Jersey e Isola di Man - , Romania, Slovacchia, Slovenia, Spagna, Svezia, Ungheria, **Svizzera** 



Cliccando sul menù a tendina *Richiedente*. si può scegliere se fare la richiesta come Privato Cittadino oppure come Legale Rappresentante Impresa. Selezionando Privato Cittadino, si visualizzerà nella schermata successiva come Ufficio di riferimento quello nella stessa provincia di

#### 1.2: Definizione parametri richiedente



KESIDENZA

Codice fiscale: GIOFRC92E65A717F

Email: federica.gioe@infocamere.it

Cellulare: +393282949107

Cognome: GIOÈ

Data di nascita: 25/05/1992

25/05/1992 **Sesso:** 

Nazione di nascita: IT Provincia di nascita: AP Comune di nascita: ALTIDONA Cittadinanza: IT

Richiedente:	Legale Rappresentante Impresa ▼	
DATI IMPRESA		
C. fiscale / P.iva	02313821007	
Provincia:	ROMA ▼	

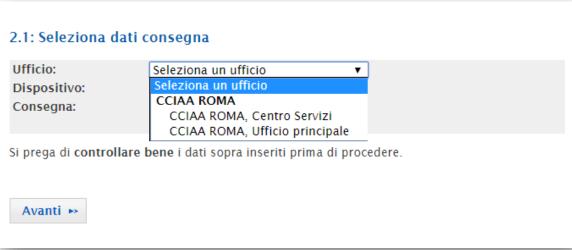
Nome:

**FEDERICA** 

Nazione:	Provincia:				
ITALIA	▼ ALESSANDRIA ▼				
Comune/Città:	CAP:				
ARQUATA SCRIVIA ▼	15121				
Indirizzo:	,				
VIA ▼	N. civico:				
ROMA	1				
DATI DOCUMENTO					
Tipo documento:	Numero Documento:				
Carta identità ▼	AA12345				
Emesso da:	Emesso il: (dd/mm/aaaa)				
COMUNE	12/12/2019				
PASSPHRASE  E' LA PASSWORD CHE SERVIRÀ PER DECIFRARE LA SCRATCH-CARD ASSOCIATA ALLA CNS CHE VERRÀ INVIATA, IN FORMATO PDF, VIA EMAIL.  NON DEVE ESSERE COMUNICATA A TERZI E VA CUSTODITA IN MODO SICURO. ÎNSERIRE DA 10 A 30 CARATTERI NUMERICI/ALFABETICI, SIA MINUSCOLI CHE MAIUSCOLI, ESCLUSI CARATTERI SPECIALI O ACCENTATI.					
Passphrase:	Conferma:				
computer1234	computer1234				
Si prega di controllare bene i dati sopra inseriti prima di procedere.					

Selezionando Legale Rappresentante Impresa, l'utente dovrà inserire nello stesso passaggio Codice fisale/Partita Iva dell'impresa e Provincia in cui l'impresa ha Sede Legale.

Nella schermata successiva l'Ufficio di riferimento sarà quello della provincia di riferimento della **sede legale** dell'impresa.





#### 2.1: Seleziona dati consegna

Ufficio: CCIAA Alessandria, Ufficio principale ▼

Consegna: Ritiro in camera ▼

Dichiaro di aver preso completa ed attenta visione del "Manuale Operativo Servizio di Certificazione Digitale" (vedi)

Dichiaro di aver preso completa ed attenta visione del "Manuale Operativo Carta Nazionale Servizi" (vedi)

Dichiaro di aver preso completa ed attenta visione e di accettare le "Condizioni Generali di Contratto" (vedi)

Dichiaro di aver preso completa ed attenta visione del modulo di richiesta (vedi)

Dichiaro di aver preso completa ed attenta visione dell'informativa Privacy per l'utilizzo della Web Identification (vedi)

Si prega di controllare bene i dati sopra inseriti prima di procedere.

Avanti 🔛

Si seleziona la tipologia di dispositivo e di consegna, infine si prende visione di una serie di **documenti:** 

- ❖ MANUALE OPERATIVO SERVIZIO DI CERTIFICAZIONE DIGITALE
- MANUALE OPERATIVO CARTA NAZIONALE DEI SERVIZI
- ❖ CONDIZIONI GENERALI DI CONTRATTO
- **♦** MODULO DI RICHIESTA
- ❖ INFORMATIVA PRIVACY PER L'UTILIZZO DELLA WEB IDENTIFICATION





Si sceglie il giorno e l'ora dell'appuntamento per il riconoscimento online in base agli slot resi disponibili dalla Camera di Commercio.

Si hanno 24 ore per concludere il pagamento, **se si dovesse uscire dalla pagina questa viene memorizzata** (check point). Una volta ritornati alla pagina di richiesta, compilato lo step 1, si verrà dirottati nel punto esatto dove si aveva abbandonato la procedura.

Avanti >>

#### 4.1: Selezione modalità di pagamento

DATI ORDINE

Richiesta: 28609

del: Token wireless DDNA Consegna:

11-03-2020 17:42 c/o CCIAA

Dispositivo: Stato:

INVIATA\_CMS

RICHIEDENTE

SARA Nome: Email: sara.pirro@infocamere.it

PIRRO Cognome: Cellulare:

3334455666

Pass-phrase:

Ciaociaociaociao1

DATI RITIRO DISPOSITIVO

Ufficio: CCIAA Alessandria, Ufficio principale

Indirizzo:

VIA prova, 1

15013

Telefono:

0123456789

RICONOSCIMENTO DE-VISU

giovedì, 12-03-2020 Prenotato per:

Orario: 08:30

RIEPILOGO PAGAMENTO

Prodotto Token Wireless DDNA Riconoscimento Web ID Totale:

€ 70.00 € 0.00 € 70,00

Prezzo

Inizia ora il processo di pagamento del servizio richiesto tramite una delle opzioni di seguito:

Metodo di pagamento: pagoPA ▼

Il pagamento tramite pagoPA necessita di una verifica preliminare. Per procedere a tale verifica, premere il pulsante qui sotto; se l'esito sarà positivo potrete procedere al pagamento del servizio.

Verifica richiesta... >>



Si ha un riepilogo della richiesta con:

- DATI ORDINE
- DATI RICHIEDENTE
- DATI RITIRO DISPOSITIVO (si è scelto in questo caso il ritiro in camera)
- RICONOSCIMENTO DE VISU (con la data e l'ora prescelti)
- RIEPILOGO PAGAMENTO (con l'importo totale da versare)

Si procede con il pagamento attraverso il nodo PagoPA

### Prima di procedere con il pagamento è necessario effettuare una verifica.

L'utente viene dirottato nella pagina del servizio di pagamento dove potrà inserire in modo sicuro i dati di fatturazione e quelli del metodo di pagamento, per poi procedere al versamento dell'importo





#### C.C.I.A.A. MILANO MONZA BRIANZA LODI

/RFB/9700000000040308/70.00/TXT/DEBITORE/GIOFRC92E65A717F/PER/PRATICA\_MOPA\_CMS 70,00€

La piattaforma PagoPA richiede un'autenticazione, debole (accesso tramite e-mail) o forte (SPID). L'autenticazione è richiesta da PagoPA per poter consultare il dettaglio della propria posizione debitoria verso l'Ente di riferimento (CCIAA), oltre allo storico dei pagamenti già effettuati con le relative ricevute di pagamento.

IT 🗸



Benvenuto nel sistema di pagamento della Pubblica Amministrazione italiana: pagoPA



Non hai SPID? Scopri di più

Entra con la tua email



#### C.C.I.A.Á. MILANO MONZA BRIANZA LÓDI



La fase di "check out" ossia di scelta dello strumento di pagamento, è governata da una componente centralizzata chiamata WISP (Wizard Interattivo di Scelta del PSP). II WISP guida l'utente alla scelta del servizio di pagamento più conveniente, esponendo prima le modalità disponibili.



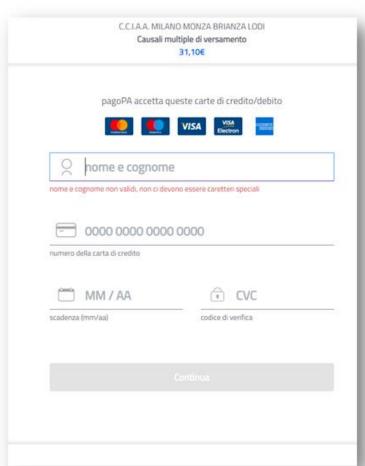
Informativa sulla privacy

#### Carta di credito/debito

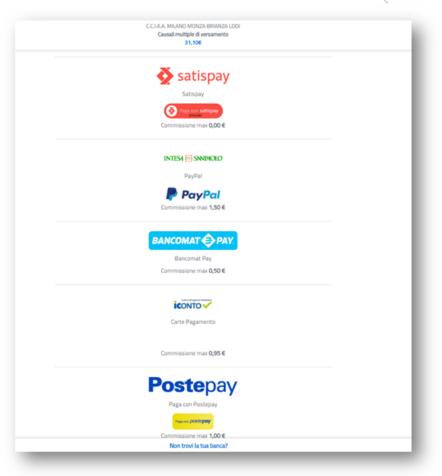
#### Conto corrente

#### Altri metodi di pagamento









Una volta selezionata lo strumento di pagamento, la piattaforma mostra i PSP (Prestatori di Servizi di Pagamento) che offrono il servizio in modo compatibile con le particolari caratteristiche della richiesta di pagamento. La componente WISP 2.0 propone la possibilità di autenticarsi per poter usufruire delle funzionalità avanzate, quali la memorizzazione del servizio di pagamento utilizzato in caso di esito positivo della transazione e il salvataggio delle credenziali, qualora l'Ente creditore abbia già identificato l'utente tramite SPID.

#### 5: Riepilogo



Verifica del pagamento: operazione effettuata con successo.

Il pagamento risulta completato con successo e la sua richiesta verrà presa in carico quanto prima dal sistema di emissione dei dispositivi (CMS).

#### STAMPI E CONSERVI IL SEGUENTE RIEPILOGO:

DATI ORDINE

Richiesta: 28609 del: 11-03-2020 17:42

Dispositivo: Token wireless DDNA Consegna: c/o CCIAA

Stato: PAGATA

RICHIEDENTE

Nome: SARA Cognome: PIRRO Email: sara.pirro@infocamere.it Cellulare: 3334455888

Pass-phrase: Ciaociaociaociao1

DATI RITIRO DISPOSITIVO

Ufficio: CCIAA Alessandria, Ufficio principale

Indirizzo: VIA prova, 1 Cap: 15013

Telefono: 0123456789

RICONOSCIMENTO DE-VISU

Prenotato per: giovedì, 12-03-2020 Orario: 08:30

RIEPILOGO PAGAMENTO

ProdottoPrezzoToken Wireless DDNA€ 70,00Riconoscimento Web ID€ 0,00Totale:€ 70,00

Le è stata inviata una mail con il riepilogo dei dati della sua richiesta; qualora non l'avesse ricevuta o desiderasse un ulteriore reinvio, clicchi sul pulsante "Invio email"

Stampa... 🚇 Invio email... 🗈



La procedura di acquisto del dispositivo è terminata e si ha la possibilità di **stampare il riepilogo.** 

Si riceve l'e-mail con il riepilogo dei dati, in caso contrario cliccare su **Invio email.** 

La ringraziamo per aver scelto i nostri servizi.



# E-mail ricevute

Terminata con successo la richiesta online si ricevono 4 e-mail:

mittente		<u>oggetto</u>
no reply noreply-pagopa no reply <b>no reply</b>	- - -	PagoPA AVVISO ESITO PAGAMENTO NUM. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX



# Il link al video riconoscimento

no-reply 6

4

Posta in arrivo WeBid Prenotazione Effettuata - b"-





#### no-reply@infocamere.it

Gentile

l'appuntamento per il suo video-riconoscimento è stato correttamente registrato.

Per iniziare la sua sessione di video-riconoscimento clicchi su questo link\*. Ricordiamo che questo link ha una validità di 30 giorni.



\*per un'ottimale fruizione del servizio si suggerisce l'utilizzo dei browser Google Chrome, Internet Explorer, Mozilla Firefox

#### Distinti Saluti

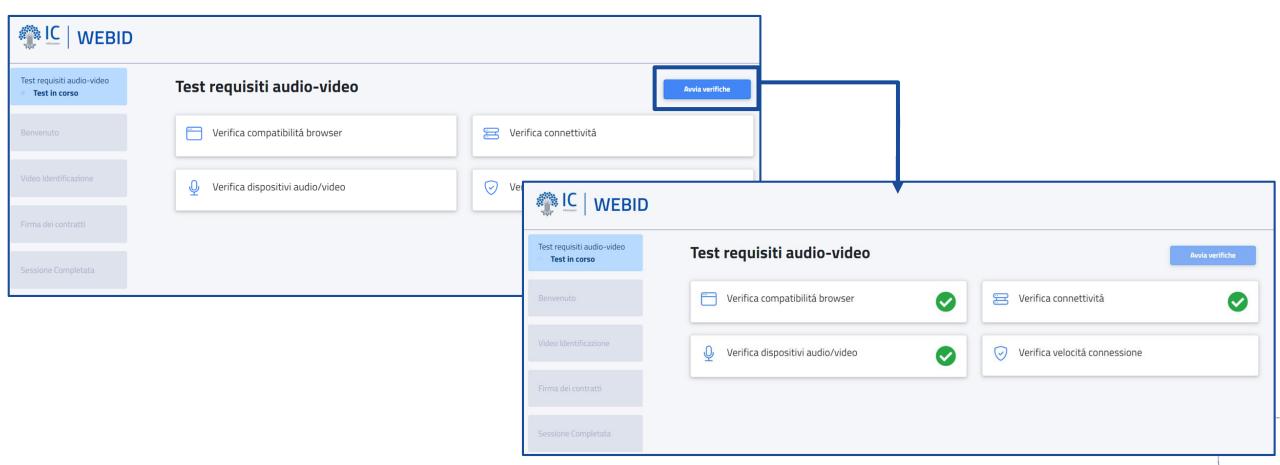
Email inviata Automaticamente

Prima di collegarsi al video riconoscimento assicurarsi di avere il documento di riconoscimento utilizzato per fare la richiesta online, il tesserino del codice fiscale/tessera sanitaria e il telefono cellulare.



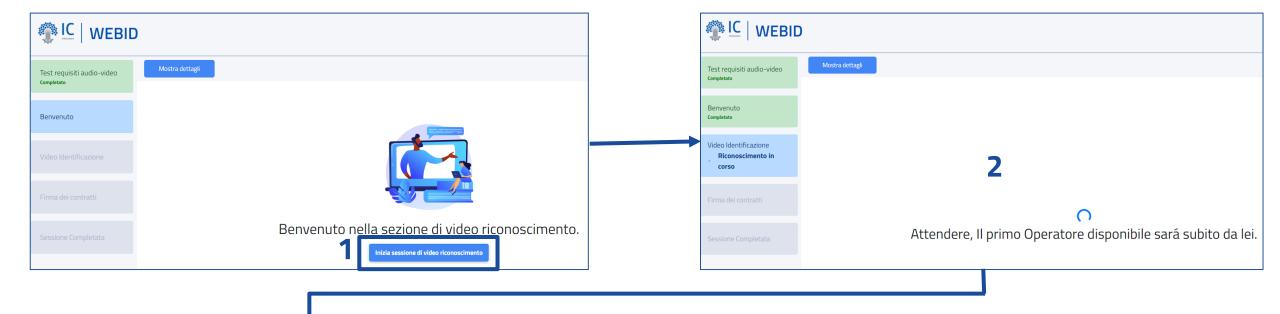
# Il video riconoscimento

All'ora e data stabilite, cliccando il **link** ricevuto nella mail a termine della richiesta online, ci **si connette alla piattaforma** di video riconoscimento. La prima operazione da fare è effettuare le **verifiche** del funzionamento di videocamera e microfono.





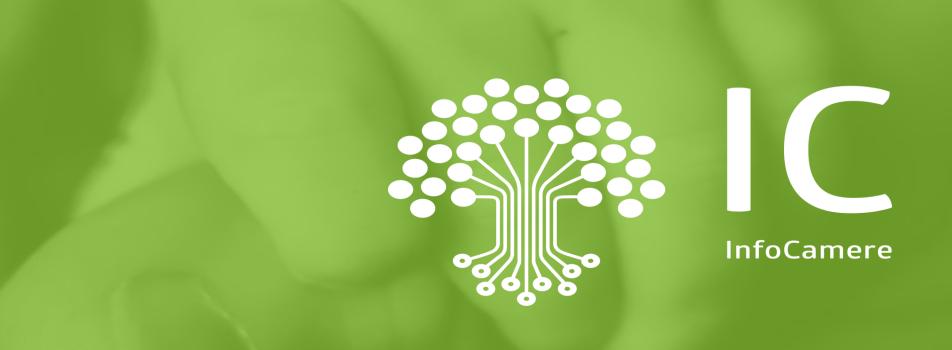
# Connessione al video riconoscimento





Dopo la verifica di microfono e videocamera, si viene indirizzati al *Benvenuto* dove si cliccherà **Inizia sessione di video riconoscimento** (1).

Si attende un operatore disponibile (2) qualora non ci sia immediatamente uno - e poi si viene collegati quando disponibile (3)



Spazio alle domande







