InfoCert
GRUPPO TECNOINVESTIMENTI

LegalCert

Linee guida identificazione autenticazione soggetto richiedente certificazione digitale

Istruzioni tecniche

1 Novità introdotte rispetto alla precedente emissione

VERSIONE/RELEASE N° :	2	**Data Versione/Release :**	12/12/2017
Descrizione modifiche:	Formato Serial Number a seguito pubblicazione Determina 189 (in vigore dal 23/12/2017)		

VERSIONE/RELEASE N° :	1	**Data Versione/Release :**	01/02/2017
Descrizione modifiche:	prima emissione		

2 Scopo e campo di applicazione del documento

Il presente documento ha lo scopo di documentare le linee guida per l'identificazione e l'autenticazione del soggetto che richiede all' Ente Certificatore l'emissione, il rinnovo e/o l'eventuale revoca/sospensione di un certificato di firma digitale

2.1 Riferimenti

- [1] Manuali Operativi Certificati, consultabili sul sito www.firma.infocert.it, sezione "Documentazione Tecnica/Manuali Operativi"
- [2] Certificate Policy dei Certificati di Autenticazione per la Carta Nazionale dei Servizi, consultabili sul sito www.firma.infocert.it, sezione "Documentazione Tecnica/ Manuali Operativi".

2.2 Termini e definizioni

TSP	Dall'espressione internazionale "Trust Service Provider", introdotta in Italia come "prestatore di servizi elettronici fiduciari", è "una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificati". (art. 3 n. 19 eIDAS)
Servizio fiduciario	un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi: a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure b) creazione, verifica e convalida di certificati di autenticazione di siti web; o c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi. (art. 3 n. 16 eIDAS).
QTSP	Dall'espressione internazionale "Qualified Trust Service Provider", introdotta in Italia come "prestatore di servizi elettronici fiduciari", è "un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato" (art. 3 n. 20 eIDAS)
Servizio fiduciario qualificato	Il servizio fiduciario che soddisfa i requisiti eIDAS (art. 3 n. 17 eIDAS)
Certificato	Insieme di informazioni atte a definire con certezza la corrispondenza tra l'identità del soggetto certificato e la sua chiave pubblica; nel certificato compaiono altre informazioni tra cui: - il Certificatore che lo ha emesso; - il periodo di tempo di validità; - altri campi (estensioni) che determinano caratteristiche aggiuntive. (Dal Manuale Operativo dell'Ente Certificatore InfoCert)
CNS	Carta Nazionale dei Servizi; per "CNS like" si intende invece una smart card con caratteristiche simili ad una CNS ma che non può contenere un certificato CNS (vedere tabella al paragrafo 3.3)

ERC	Acronimo di Emergency Request Code, codice di emergenza
IUT	Identificativo Univoco Titolare. È composto da: 1) Anno (4 ch) di registrazione richiesta certificato; 2) Ufficio (6 ch) identificativo interno ufficio di registrazione di appartenenza dell'user autenticata che ha effettuato la registrazione richiesta certificato; 3) A (fisso 1 ch) eventuale per i soli certificati non di firma. Progressivo (ch variabile) registrazione richiesta certificato; 4) Il progressivo è annuale per ufficio di registrazione. Es. 200711111115 (quindicesima registrazione per l'ufficio 111111 nell'anno 2007 di tipo sottoscrizione) 2007111111A15 (quindicesima registrazione per l'ufficio 111111 nell'anno 2007 di tipo autenticazione)
Firma digitale	Per definizione: "un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici" (art. 1 comma 1 lettera s D.lgs 7 marzo 2005 n. 82 – CAD)
Frame	Regioni distinte della finestra del Browser. Con questa tecnica è possibile in una regione passare ad una pagina html lasciando l'altra inalterata
Look Up	Tabella di codici. Generalmente sui campi che prevedono un codice è possibile attivare, mediante click sul pulsante vicino, la visualizzazione dei codici permessi e scegliere il codice desiderato.
Oggetto	Qualsiasi oggetto della videata. I più importanti sono i campi da digitare, i pulsanti, i collegamenti (parti del testo sottolineate e/o colorate in modo diverso). Generalmente i pulsanti indicano un'azione (es. Registra, etc..), i collegamenti la richiesta di altre videate dell'applicazione.
PIN	Personal Identification Number, codice associato ad un dispositivo sicuro di firma, utilizzato dal Titolare per accedere alle funzioni del dispositivo stesso
PUK	Personal Unlocking Key – codice di sblocco del dispositivo sicuro di firma
RAO	Registration Authority Officer - Operatore dell'Ufficio di Registrazione: soggetto incaricato a verificare l'identità e, se applicabile, ogni specifico attributo di un Titolare, nonché ad attivare la procedura di certificazione per conto del Certificatore. (Dal Manuale Operativo dell'Ente Certificatore InfoCert)
IR	Incaricato della Registrazione, soggetto facente capo ad un determinato Ufficio di Registrazione, che effettua la sola identificazione dell'Utente Titolare e ne annota i dati necessari (su apposito modulo cartaceo, o in alternativa in una maschera via Internet)
Smart Card	Il dispositivo sicuro di firma utilizzato dal Titolare, è costituito da una carta di plastica delle dimensioni di una carta di credito in cui è inserito un microprocessore. È chiamato anche **carta a microprocessore.** Rispetta i requisiti di sicurezza richiesti dalla normativa vigente. (DPCM 22/02/2013)
Store di Microsoft	Si intende quell'area di memoria del S.O. dove vengono memorizzati i certificati digitali.

TIN	E' un acronimo che sta per "*Tax Identification Number*", ovvero un codice di 9 cifre che corrisponde al nostro codice fiscale
Token USB	Dispositivo in formato chiave USB, che abbina la funzione di una smart card e del suo lettore
Ufficio di Registrazione	Entità che esegue le operazioni di autenticazione, identificazione, raccolta e conservazione dei dati relativi ai richiedenti i certificati
Utente Titolare	Utente finale possessore della Smart Card o del Token USB e titolare del certificato.

Numero di Serie (Serial Number)

A seguito della pubblicazione della Determina 189 (in vigore da 23/12/2017) varia il formato come di seguito descritto.

Il Serial Number deve essere valorizzato in assenza del codice fiscale italiano.

Il Serial Number deve avere il seguente formato

>>tipo identificativo 3 octet>>-<<codice identificativo>>

I cui valori possibili sono:

Tipo Identificativo	Codice Identificativo	Note
PAS	Numero passaporto	
IDC	Numero carta identità 'nazionale'	
PNO	Numero registrazione personale 'nazionale'	
RP	Permesso di soggiorno	Da usare solo con CountryCode IT
NS	Identificativo assegnato in modo univoco dalla Registration Authority	Da usare solo con CountryCode diverso da IT

(TIN continua ad essere utilizzato per il codice fiscale)

Di seguito alcuni esempi:

PAS-P5665545566

IDC-UG34344FD

PAS-G244355444

RP-2334335654333

NS-gkj5675

3 Identificazione e autenticazione per l'emissione dei certificati

3.1 Denominazione

3.1.1 Tipi di nomi

Il soggetto nel certificato è identificato con l'attributo Distinguished Name (DN) che quindi deve essere valorizzato e conforme lo standard X509. I certificati vengono emessi secondo gli standard ETSI per l'emissione dei certificati qualificati [412] e secondo le indicazioni presenti nel DPCM.

3.1.2 Necessità che il nome abbia un significato

L'attributo del certificato Distinguished Name (DN) identifica in maniera univoca il soggetto a cui è rilasciato il certificato.

3.1.3 Anonimato e pseudonimia dei richiedenti

Solo in caso di identificazione secondo la modalità 1_LiveID (vedi 3.2.3) è facoltà del Soggetto richiedere alla CA che il certificato riporti uno pseudonimo in luogo dei propri dati reali. Poiché il certificato è qualificato, la CA conserverà le informazioni relative alla reale identità dell'utente per venti (20) anni dall'emissione del certificato stesso.

3.1.4 Regole di interpretazione dei tipi di nomi

InfoCert si attiene allo standard X509.

3.1.5 Univocità dei nomi

Nel caso di persona fisica, per garantire l'univocità del Soggetto, nel certificato deve essere indicato il nome e cognome e un codice identificativo univoco:

- il Codice Fiscale se il soggetto ne è in possesso;
- altro codice identificativo negli altri casi: può essere stato assegnato dalle autorità del Paese di cui il Soggetto è cittadino ovvero dal Paese in cui ha la sede l'organizzazione in cui esso lavora.
-

Pre-attivazione Determina 189:
In assenza di Codice Fiscale, nel certificato potrà essere inserito un codice identificativo tratto da un documento di identità valido, utilizzato nell'ambito delle procedure di riconoscimento.

Post-attivazione Determina 189:
In assenza di Codice Fiscale, nel certificato potrà essere inserito un codice identificativo (uno tra PAS, IDC, PNO, RP, NS descritti in 2.2) tratto da un documento di identità valido, utilizzato nell'ambito delle procedure di riconoscimento.

Nel caso di persona giuridica, per garantire l'univocità del soggetto, nel certificato deve essere indicato il nome dell'organizzazione e un codice identificativo univoco:

- la Partita IVA o il Numero di Registro Imprese per le persone giuridiche italiane,
- i codici VAT (Value Added Tax Code) o NTR (National Trade Register) per le persone giuridiche.

3.1.6 Riconoscimento, autenticazione e ruolo dei marchi registrati

Il Soggetto e il Richiedente, quando richiedono un certificato alla CA garantiscono di operare nel pieno rispetto delle normative nazionali e internazionali sulla proprietà intellettuale.

La CA non fa verifiche sull'utilizzo di marchi, e può rifiutarsi di revocare un certificato coinvolto in una disputa.

3.2 Convalida iniziale dell'identità

Questo capitolo descrive le procedure usate per l'identificazione del Soggetto o del Richiedente al momento della richiesta di rilascio del certificato qualificato.

La procedura di identificazione comporta che il Soggetto sia riconosciuto dalla CA, anche attraverso la RA o un suo Incaricato, che ne verificherà l'identità attraverso una delle modalità definite nel Manuale Operativo.

3.2.1 Metodo per dimostrare il possesso della chiave privata

InfoCert stabilisce che il richiedente possiede o controlla la chiave privata corrispondente alla chiave pubblica da certificare, verificando la firma con la chiave pubblica da certificare

3.2.2 Autenticazione dell'identità delle organizzazioni

n/a

3.2.3 Identificazione

Ferma restando la responsabilità della CA, l'identità del Soggetto viene accertata dai soggetti abilitati a eseguire il riconoscimento, attraverso le seguenti modalità:

Modalità	Soggetti abilitati a eseguire l'identificazione	Strumenti di autenticazione a supporto della fase di identificazione
1 LiveID	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione • Pubblico Ufficiale • Datore di Lavoro per la identificazione dei propri dipendenti, collaboratori, agenti	n/a
2 AMLID	• Soggetti destinatari degli obblighi Antiriciclaggio ai sensi delle normative di recepimento della Direttiva 2005/60/CE del Parlamento Europeo e del Consiglio relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, e delle successive normative comunitarie di esecuzione • In Italia, soggetti destinatari degli obblighi Antiriciclaggio ai sensi del D.Lgs 231/2007 e smi, Capo III	n/a
3 SignID	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione	Utilizzo di una firma elettronica qualificata emessa da un Prestatore di Servizi Fiduciari Qualificato
4 AutID	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione	• Utilizzo di un dispositivo CNS o TS-CNS in corso di validità • Utilizzo di un dispositivo CIE in corso di validità • Utilizzo di una identità SPID di livello 3, in corso di validità e emessa da un Gestore di Identità Digitale SPID • Utilizzo di una identità proveniente da altri sistemi di identificazione informatica ritenuti conformi ai requisiti dello SPID • Utilizzo di una eID di livello 4 in corso di validità emessa da un Prestatore Qualificato di Servizi Fiduciari
5 VideoID	• Certification Authority (CA) • Registration Authority (RA)	n/a

	• Incaricato alla Registrazione	

3.2.3.1 Riconoscimento effettuato secondo la modalità 1 - LiveID

La modalità di identificazione **LiveID** prevede un incontro di persona tra il Soggetto, che deve aver compiuto 18 anni di età, e uno dei soggetti abilitati a eseguire il riconoscimento, che provvede ad accertare la sua identità mediante l'esibizione in originale di uno o più documenti d'identificazione in corso di validità[1]. Il Soggetto deve essere in possesso anche del Codice Fiscale, la cui esibizione può essere richiesta dal soggetto abilitato a eseguire il riconoscimento. I soggetti privi di codice fiscale italiano devono esibire il documento contenente un analogo codice identificativo (par 2.2).

L'identificazione può essere eseguita anche da parte di un Pubblico Ufficiale in base a quanto disposto dalle normative che disciplinano la loro attività. Il Soggetto compila la richiesta di Certificazione e la sottoscrive di fronte a un Pubblico Ufficiale, facendo autenticare la propria firma ai sensi delle normative vigenti. La richiesta è poi presentata alla CA a uno degli Uffici di Registrazione convenzionati.

L'identificazione già eseguita dal datore di lavoro ai fini della stipula del contratto di lavoro è considerata valida dalla CA in conformità alla seguente modalità di riconoscimento. Analogamente, è considerata valida in conformità alla seguente modalità di riconoscimento:

- l'identificazione eseguita dal datore di lavoro nell'ambito della attivazione di rapporti di agenzia
- l'identificazione eseguita dal datore di lavoro dei già dipendenti in stato di pensione, che continuano ad accedere ai portali e/o ai locali aziendali per esigenze ricreative, o di agevolazioni su beni e servizi, previsti dagli accordi aziendali.

I dati di registrazione per la modalità di identificazione LiveID sono conservati dalla CA in formato analogico o in formato elettronico.

3.2.3.2 Riconoscimento effettuato secondo la modalità 2 - AMLID

Nella **modalità 2 - AMLID** la CA si avvale dell'identificazione eseguita da uno dei soggetti destinatari degli obblighi di Identificazione e Adeguata Verifica, ai sensi delle normative tempo per tempo vigenti, di recepimento della Direttiva 2005/60/CE del Parlamento Europeo e del Consiglio relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, e delle successive ulteriori normative comunitarie di esecuzione.

Con specifico riferimento al contesto italiano, i dati utilizzati per il riconoscimento sono rilasciati dal Soggetto ai sensi del D.Lgs. 231/2007 e s.m.i., a norma del quale i clienti sono tenuti a fornire - sotto la propria

[1] Per l'Italia sono i documenti previsti dal DPR 445/2000 e s.m.i. (Testo Unico Documentazione Amministrativa). I titolari con cittadinanza diversa da quella italiana, ai fini dell'identificazione esibiscono in originale uno dei seguenti documenti d'identificazione:

- passaporto,
- carta di identità italiana (se cittadini europei).

La CA si riserva la facoltà di accettare documenti di identità emessi da autorità di Paesi appartenenti alla Unione Europea, sulla base della analisi delle caratteristiche oggettive di certezza dell'identità e sicurezza nel processo di emissione dei documenti stessi da parte della Autorità Emittenti

responsabilità - tutte le informazioni necessarie e aggiornate per consentire ai Soggetti destinatari degli Obblighi elencati nel Capo III della predetta norma, di adempiere agli obblighi di identificazione della clientela. I soggetti destinatari degli obblighi acquisiscono i dati in base alle procedure definite in autonomia nel rispetto di quanto previsto dal Titolo II e dal Titolo III del D.Lgs. 231/2007 e s.m.i., ovvero alle analoghe procedure adottate secondo le norme antiriciclaggio vigenti alla data del riconoscimento (anche se in epoca anteriore al presente Manuale).

Questa modalità di identificazione prevede il conferimento da parte della CA di un mandato con rappresentanza al soggetto destinatario degli obblighi, che agisce quindi da RA. I dati identificativi del Soggetto raccolti all'atto del riconoscimento sono conservati dalla CA di norma in modalità elettronica e possono essere conservati anche in modalità analogica

3.2.3.3 Riconoscimento effettuato secondo la modalità 3 - SignID

Nella **modalità 3 SignID** la CA InfoCert si basa sul riconoscimento già effettuato da un'altra CA che emette certificati qualificati**.** Il Soggetto è già in possesso di un certificato qualificato ancora in corso di validità, che utilizza nei confronti di InfoCert. I dati di registrazione sono conservati, in questo caso, esclusivamente in formato elettronico.

3.2.3.4 Riconoscimento effettuato secondo la modalità 4 - AUTID

Nella **modalità 4 AutID** la CA si basa sul riconoscimento già effettuato alternativamente dai seguenti soggetti:

- Ente Emettitore di CNS (Carta nazionale dei Servizi) o TS-CNS (Tessera Sanitaria – Carta Nazionale dei Servizi)
- Comune che ha rilasciato la CIE (Carta di Identità Elettronica)
- Gestore di Identità Digitale SPID (Sistema Pubblico di Identità Digitale SPID)
- Identiy Provider eID eIDAS

Il Soggetto deve essere quindi in possesso di un dispositivo sicuro con un certificato CIE o CNS ancora in corso di validità, ovvero di una identità SPID di livello 3 o di una eID eIDAS LoA 4, con la quale si autentica ai sistemi della CA o della RA che ne accerta così la identità.

Si considera coerente con la presente modalità di identificazione l'utilizzo di una identità proveniente da altri sistemi di identificazione informatica ritenuti conformi ai requisiti dello SPID, il cui uso ai fini dell'ottenimento di una identità SPID sia stato preventivamente autorizzato da AgID secondo le procedure previste.

I dati di registrazione sono conservati, in questi casi, esclusivamente in formato elettronico.

3.2.3.5 Riconoscimento effettuato secondo la modalità 5 - VideoID

Nella **modalità 5 VideoID** è richiesto al Soggetto il possesso di un device in grado di collegarsi a internet (PC, smartphone, tablet, etc.), una webcam e un sistema audio funzionante.

L'Incaricato alla Registrazione verifica l'identità del Soggetto o del Richiedente tramite il riscontro con uno o più documenti di riconoscimento in corso di validità, purché muniti di fotografia recente e riconoscibile.

Per ragioni di sicurezza e procedure anti-frode, il tipo di documenti accettati da questa modalità è limitato ai documenti di identità maggiormente diffusi (come ad esempio la carta di identità, la patente, il passaporto)[2]. È facoltà dell'Incaricato alla Registrazione escludere l'ammissibilità del documento utilizzato dal Soggetto o dal Richiedente se ritenuto carente delle caratteristiche elencate. I dati di registrazione, costituiti da file audio-video e metadati strutturati in formato elettronico, sono conservati in forma protetta.

Di seguito una descrizione dettagliata dei controlli standard che l'operatore incaricato per questo tipo di riconoscimento deve effettuare al fine del buon esito dello stesso.

3.2.3.5.1 Controlli generali riconoscimento modalità 5 - VideoID

Verifica preliminare dell'identità

Prima di procedere con il riconoscimento, nella fase di welcome, l'operatore si assicura che l'utente sia colui che ha prenotato la sessione. Questo controllo è effettuato mediante una domanda di conferma diretta all'utente della corrispondenza del nome e cognome, numero di telefono, estremi del documento di identità la data e l'ora al momento della verifica preliminare.

Se si presenta un utente diverso, a causa di un errore con le prenotazioni il riconoscimento non avrà inizio.

Controllo condizioni di luce ottimali e posizione utente

Sin dall'inizio della sessione, l'operatore si assicura che le condizioni di luce siano ottimali e chiudere/aprire fonti di luce in previsione delle foto che dovrà scattare di lì a poco.

Foto nitide

Al momento di scattare le foto, avendo previamente ottimizzato le condizioni di luce, l'operatore chiederà all'utente di prestare attenzione e rimanere fermo al fine di scattare foto il più nitide possibile.

In caso di foto sfocate, a meno che ciò non sia dovuto alla scarsa risoluzione della webcam, l'operatore potrà chiedere all'utente di riposizionarsi per un altro scatto.

Se necessario, l'operatore potrà scattare anche foto dei dettagli dei documenti, garantendo la visibilità delle informazioni oggetto di controllo (es. timbro dell'autorità che lo ha rilasciato, data scadenza, ecc).

[2] La CA si riserva la facoltà di accettare ulteriori tipologie di documenti di identità, ovvero documenti emessi da autorità di Paesi appartenenti alla Unione Europea, sulla base della analisi delle caratteristiche oggettive di certezza dell'identità e sicurezza nel processo di emissione dei documenti stessi da parte della Autorità Emittenti.

3.2.3.5.2 Controlli generici documenti riconoscimento modalità 5 - VideoID

Di seguito una serie di controlli e accortezze che l'operatore dovrà adottare indipendentemente dal tipo di documento presentato.

- Deve sempre essere presente sul documento la sottoscrizione autografa del cliente.
- Il documento presentato dovrà essere in corso di validità, quindi l'operatore avrà cura di controllare la data di scadenza.
- Il volto dell'utente e le relative foto devono corrispondere: per questo tipo di controllo ci si rifà al buon senso dell'operatore, lo stesso che usano gli ufficiali dell'anagrafe al momento del rilascio dei documenti di identità e per il loro rinnovo.
- Ogni documento deve presentare, ben visibili, tutti i dati oggetto di verifica oltre al timbro dell'autorità che lo ha emesso, ove presente.
- Se effettuando le verifiche dovesse emergere una difficoltà nel verificare la validità dei dati presenti sul documento presentato (es. inchiostro sbiadito; foto sbiadita; ecc.), dovrà essere proposto al cliente di presentare un differente documento di identità, tra quelli ammessi.
- Dovrà essere verificato che il NOME e COGNOME dichiarati dal cliente, corrispondano perfettamente con quelli presenti sul Documento di Identità presentato e che il codice fiscale/identificativo riportato corrisponda con quello presente sulla tessera del codice fiscale/identificativo.
- L'utente deve sempre presentare i documenti in originale. Nel particolare caso in cui l'utente non ne sia in possesso per cause a lui non imputabili e allo stesso tempo dichiari di non poter godere di un diritto irrinunciabile in assenza di identità SPID, è ammissibile accettare, quali sostitutivi cartacei temporanei dei documenti, la fotocopia del documento di identità e la Tessera Sanitaria cartacea temporanea.
  In combinato alla presentazione della fotocopia della carta di identità, è necessario richiedere la presentazione dell'originale della denuncia di smarrimento non antecedente a 20 giorni. In questo caso si dovrà informare l'utente dell'obbligo di produrre entro e non oltre due giorni lavorativi un documento di identità in corso di validità, pena la revoca dell'identità. Contestualmente l'operatore notificherà ad InfoCert l'avvenuto riconoscimento dell'utente segnalandone lo stato di "attesa documento in originale".

3.2.3.5.3 Controlli specifici documenti riconoscimento modalità 5 – VideoID

Carta di identità

Di seguito tutti i tipi di controlli che l'operatore dovrà effettuare sulla carta di identità e le varie casistiche in base all'esperienza InfoCert:

- Non perfettamente leggibile: dovrà chiedere un altro documento.
- L'utente si presenta con un indumento che gli nasconde parte dei lineamenti del viso: l'operatore dovrà chiedere gentilmente all'utente di mostrare il volto. In caso l'utente sia anche provvisto di carta di identità in cui non sono visibili i tratti del volto, non si può procedere all'identificazione.
- CIE con validità estesa, il cui timbro di estensione è apposto su un allegato cartaceo: è necessario fotografare anche l'allegato cartaceo.
- Può essere accettata la sola Carta d'Identità ITALIANA

Tipo doc.	Controllo	Applicativo	Manuale	Livello di warning
CI	Presenza della firma autografa del titolare		X	3
CI	Font numero di serie corrispondente allo standard del Poligrafico della Zecca dello Stato		X	3
CI	Presenza e leggibilità del timbro a secco o a inchiostro su foto del titolare		X	2
CI	Presenza e leggibilità del timbro a secco o a inchiostro e corrispondenza araldica dell'Ente emittente		X	2
	Presenza e leggibilità del timbro a secco o a inchiostro del PU che ha rilasciato il documento		X	2
CI	Estremi atto di nascita conformi alle direttive di rilascio documenti: non presenza per i nati all'estero, stampa degli estremi corrispondente alle celle		X	2
CI	Bordatura corrispondente allo standard del Poligrafico della Zecca dello Stato		X	2
CIE	Presenza della firma autografa del titolare		X	3
CIE	Presenza chip		X	3
CIE	Presenza ologramma		X	3
CIE	Presenza banda magnetica		X	3

In caso di livello di warning 2, l'operatore dovrà attuare il seguente comportamento: richiedere un secondo documento tra quelli della lista al paragrafo 2.2.1.

in caso di livello di warning 3, l'operatore dovrà attuare il seguente comportamento: dichiarare il KO della sessione ed informare l'Utente che non è possibile procedere all'identificazione.

Tessera Sanitaria

Di seguito tutti i tipi di controlli che l'operatore dovrà effettuare sul codice fiscale e le varie casistiche in base all'esperienza InfoCert:

- Tessera sanitaria sul cui retro sono presenti asterischi: in caso l'utente non sia in grado di fornire altra tessera per il codice fiscale, non è possibile procedere all'identificazione e lo si invita ad utilizzare un'altra modalità di riconoscimento.
- È accettata esclusivamente la Tessera Sanitaria italiana.
- La Tessera Sanitaria scaduta non può essere accettata.
- L'utente presenta il foglio cartaceo sostitutivo: è possibile accettare tale tipo di documento.
- L'utente non possesso di TS in qualità di cittadino residente in un Paese extra UE e non assistito dal SSN, può presentare il CF provvisto del timbro apposto dal Consolato italiano in sostituzione della TS.

Tipo documento	Controllo	Applicativo	Manuale	Livello di warning
TS	Presenza di asterischi sul retro		X	3
TS	Presenza codice braille		X	3

Patente

Di seguito tutti i tipi di controlli che l'operatore dovrà effettuare sulla patente e le varie casistiche in base all'esperienza InfoCert:

- Tessera plastificata con retro non leggibile: l'importante è che la data di scadenza, sul fronte, sia leggibile e valida. È comunque necessario fotografare anche il retro.
- Può essere accettata la sola Patente ITALIANA.

Tipo documento	Controllo	Applicativo	Manuale	Livello di warning
PT cartacea	Allineamento dati anagrafici		X	3
PT cartacea	Presenza e visibilità del timbro dell'Autorità emittente e corrispondenza dell'araldica		X	2

In caso di livello di warning 2, l'operatore dovrà attuare il seguente comportamento: richiedere un secondo documento tra quelli della lista al paragrafo 2.2.1.

in caso di livello di warning 3, l'operatore dovrà attuare il seguente comportamento: dichiarare il KO della sessione ed informare l'Utente che non è possibile procedere all'identificazione.

Passaporto

Anche per il passaporto, come per tutti gli atri tipi di documento, sono necessarie almeno due foto. Nel caso di questo specifico documento, verrà raccolta la foto del fronte e quella/e della/e pagina/e contenente/i dati anagrafici e di cittadinanza e la Firma del Titolare.

Tipo documento	Controllo	Applicativo	Manuale	Livello di warning
PS	Presenza dell'immagine che attesta la presenza del microchip interno (dal 26 ottobre 2006)		X	3

In caso di livello di warning 2, l'operatore dovrà attuare il seguente comportamento: richiedere un secondo documento tra quelli della lista al paragrafo 2.2.1.

in caso di livello di warning 3, l'operatore dovrà attuare il seguente comportamento: dichiarare il KO della sessione ed informare l'Utente che non è possibile procedere all'identificazione.

3.2.4 Identificazione persona giuridica

La richiesta di certificato per persona giuridica deve essere effettuata da una persona fisica identificata in una delle modalità descritte sopra.

Deve inoltre presentare la documentazione relativa alla persona giuridica e la documentazione che attesti la sua elegibilità alla richiesta. Vd paragrafo 4.2.1

3.2.5 Informazioni del Soggetto o del Richiedente non verificate

Il Soggetto può ottenere, direttamente o con il consenso dell'eventuale Terzo Interessato, l'inserimento nel certificato di informazioni relative a:

- Titoli e/o abilitazioni Professionali;
- Poteri di Rappresentanza di persone fisiche;
- Poteri di Rappresentanza di persone giuridiche o appartenenza alle stesse;
- Esercizio di Funzioni Pubbliche, Poteri di Rappresentanza di organizzazioni ed enti di diritto pubblico o appartenenza agli stessi.

Il certificato con il **Ruolo** è conforme a quanto indicato nella Deliberazione 45 del CNIPA.

Il Soggetto deve produrre la dichiarazione idonea a dimostrare l'effettiva sussistenza dello specifico Ruolo anche attestandolo mediante Autocertificazione[3]. La CA non assume alcuna responsabilità, salvo i casi di dolo o colpa grave, in merito all'inserimento nel certificato delle informazioni autocertificate dal Soggetto.

La ragione sociale o la denominazione e il codice identificativo dell'**Organizzazione** saranno invece riportate nel certificato se essa ha autorizzato il rilascio del certificato al Soggetto, anche senza l'esplicita indicazione di un ruolo. In tale ipotesi la CA effettua un controllo sulla regolarità formale della documentazione presentata dal Soggetto. La richiesta di certificati con l'indicazione del Ruolo e/o dell'Organizzazione può provenire solo da organizzazioni in possesso di Codice Fiscale o Partita IVA, ovvero VAT Code.

3.2.6 Validazione dell'autorità

La CA ovvero la RA verificano le informazioni richieste (vd 3.2.3 e 3.2.4) per l'identificazione e validano la richiesta.

[3] Nel caso in cui la richiesta di inserimento del ruolo nel certificato sia stata effettuata mediante la sola autocertificazione da parte del Soggetto, il certificato non riporterà informazioni inerenti l'organizzazione a cui potrebbe eventualmente essere legato il ruolo stesso.

4 Identificazione e autenticazione per il rinnovo delle chiavi e dei certificati

4.1 Identificazione e autenticazione per il rinnovo delle chiavi e dei certificati

Questo paragrafo descrive le procedure usate per l'autenticazione e identificazione del Soggetto nel caso di rinnovo del certificato qualificato di firma.

Il certificato contiene al suo interno l'indicazione del periodo di validità nel campo "validità" (validity) con gli attributi "valido dal" (not before) e "valido fino al" (not after). Al di fuori di questo intervallo di date, comprensive di ore, minuti e secondi, il certificato è da considerarsi non valido.

Il Soggetto può, tuttavia, rinnovarlo, prima della sua scadenza, utilizzando gli strumenti messi a disposizione dalla CA, che presentano una richiesta di rinnovo che viene sottoscritta con la chiave privata corrispondente alla chiave pubblica contenuta nel certificato da rinnovare. Dopo la revoca o la scadenza del certificato non è possibile eseguire il rinnovo del certificato, diventando quindi necessaria una nuova emissione.

5 Identificazione e autenticazione per le richieste di revoca o sospensione

La revoca o sospensione del certificato può avvenire su richiesta del Soggetto o del Richiedente (Terzo Interessato nel caso in cui quest'ultimo abbia espresso il suo consenso per l'inserimento del Ruolo) ovvero su iniziativa della CA.

5.1 Richiesta da parte del Soggetto

Il soggetto può richiedere la revoca o sospensione compilando e sottoscrivendo anche digitalmente il modulo presente sul sito del certificatore.

La richiesta di sospensione può essere fatta attraverso un form Internet, in tal caso il Soggetto si autentica fornendo il codice di emergenza consegnato al momento dell'emissione del certificato, oppure con un altro sistema di autenticazione descritto nella documentazione contrattuale consegnata all'atto della registrazione.

Se la richiesta viene fatta presso la Registration Authority, l'autenticazione del Soggetto avviene con le modalità previste per l'identificazione.

Nel caso in cui il Soggetto sia una persona giuridica, la richiesta di sospensione o revoca deve essere eseguita da un legale rappresentante o un soggetto munito di apposita procura.

5.1.1 Richiesta da parte del Richiedente

Il Richiedente che richiede la revoca o sospensione del certificato del Soggetto si autentica sottoscrivendo l'apposito modulo di richiesta di revoca o sospensione messo a disposizione dalla CA. La richiesta dovrà essere inoltrata alla CA che si riserva di individuare ulteriori modalità di inoltro della richiesta di revoca o sospensione del Richiedente o del Terzo Interessato in apposite convenzioni da stipulare con lo stesso.