InfoCert

PRIMO ENTE
CERTIFICATORE IN ITALIA

Corso di formazione
per gli Addetti dell'Ufficio di Registrazione

Agenda

09,30 – 09,45	Presentazione contenuti della giornata
09,45 – 10,30	Panoramica sulla normativa relativa alla firma digitale
10,30 – 11,15	Gli Uffici di Registrazione - regole
11,15 – 11,30	*Pausa caffè*
11,30 – 12,30	Gli Uffici di Registrazione - procedure
12,30 – 13,00	Registrazione dati RAO
13,00 – 14,00	*Pausa pranzo*
15,00 – 17,00	L'applicativo per il rilascio dei certificati
17,00 – 17,30	Test abilitativo, lettere di nomina, attestati

Obiettivi del corso

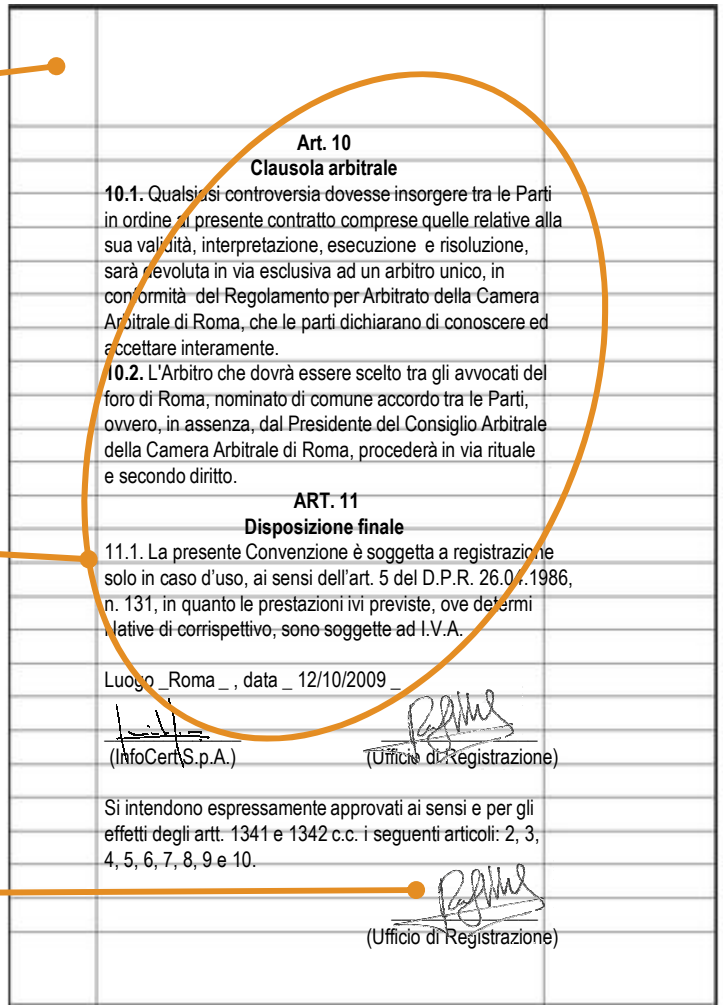
Fornire gli elementi di base tecnico-procedurali e le informazioni che permettano l'attività del RAO, la figura professionale responsabile della gestione di un Ufficio di Registrazione (RA), finalizzata all'emissione di certificati digitali e al rilascio di dispositivi di firma digitale.

Perché ci serve una firma

Supporto materiale
la carta

Il contenuto
l'informazione trasmessa

L'attribuzione a un soggetto
la firma



Art. 10
Clausola arbitrale

10.1. Qualsiasi controversia dovesse insorgere tra le Parti in ordine al presente contratto comprese quelle relative alla sua validità, interpretazione, esecuzione e risoluzione, sarà devoluta in via esclusiva ad un arbitro unico, in conformità del Regolamento per Arbitrato della Camera Arbitrale di Roma, che le parti dichiarano di conoscere ed accettare interamente.

10.2. L'Arbitro che dovrà essere scelto tra gli avvocati del foro di Roma, nominato di comune accordo tra le Parti, ovvero, in assenza, dal Presidente del Consiglio Arbitrale della Camera Arbitrale di Roma, procederà in via rituale e secondo diritto.

ART. 11
Disposizione finale

11.1. La presente Convenzione è soggetta a registrazione solo in caso d'uso, ai sensi dell'art. 5 del D.P.R. 26.0[illegible].1986, n. 131, in quanto le prestazioni ivi previste, ove determi[illegible]lative di corrispettivo, sono soggette ad I.V.A.

Luogo _Roma _ , data _ 12/10/2009 _

(InfoCert S.p.A.) (Ufficio di Registrazione)

Si intendono espressamente approvati ai sensi e per gli effetti degli artt. 1341 e 1342 c.c. i seguenti articoli: 2, 3, 4, 5, 6, 7, 8, 9 e 10.

(Ufficio di Registrazione)

Perché ci serve una firma digitale

Supporto materiale
scompare! il documento è fatto di **bit**

Il contenuto
non cambia

L'attribuzione a un soggetto
la firma diventa elettronica

Tutto iniziò…

Legge numero 59/1997 - "Legge Bassanini"

"Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa"

Articolo 15 comma 2 – Valore della firma digitale nel tempo

2. gli atti, dati e documenti formati dalla Pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge

Evoluzione del quadro normativo

firma nella CE

Direttiva 1999/93/CE > Quadro di riferimento europeo per le firme elettroniche.

Decreto Legislativo 23/01/2002 n.10 > Legge di attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche

Decreto del Presidente della Repubblica 07/04/2003 n. 137 > Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, n. 10.

Evoluzione del quadro normativo

regolamenti

Decreto del Presidente della Repubblica 10/11/1997 n. 513

Regolamento contenente i criteri e le modalità di applicazione dell'articolo 15, comma 2, della legge 15/03/1997 n. 59 in materia di formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici

Deliberazione CNIPA17/02/2005 n. 4

Regole per il riconoscimento e la verifica del documento informatico.

Deliberazione CNIPA 21/05/2009 n. 45

Regole tecnologiche di firma digitale e validazione temporale.

Evoluzione del quadro normativo

regole tecniche

Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999	Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.
Decreto del Presidente del Consiglio dei Ministri 13/01/2004	Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.
Decreto del Presidente del Consiglio dei Ministri 30/03/2009	Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.
Decreto della Presidenza del Consiglio dei Ministri 22/02/2013	Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.

Evoluzione del quadro normativo

firma remota

Decreto della Presidenza del Consiglio dei Ministri 10/02/2010

Fissazione del termine che autorizza l'autocertificazione circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza.

Decreto della Presidenza del Consiglio dei Ministri 19/07/2012

Definizione dei termini di validità delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al DPCM 30/10/2003.

Evoluzione del quadro normativo

armonizzazione degli interventi

Decreto del Presidente della Repubblica 28/12/2000 n. 445

Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

Decreto Legislativo 07/03/2005 n. 82

Codice dell'Amministrazione Digitale. Elementi per definire e garantire la validità dei documenti informatici e precisi obblighi per la loro accettazione.

Decreto Legislativo 04/04/2006 n. 159

Disposizioni integrative e correttive al Decreto Legislativo 07/03/2005 n. 82, recante Codice dell'Amministrazione Digitale.

Decreto Legislativo 30/12/2010 n. 235

Modifiche ed integrazioni al Decreto Legislativo 07/03/2005 n. 82, recante Codice dell'Amministrazione Digitale

Elementi della firma elettronica

Di cosa c'è bisogno per apporre una firma elettronica?

Elemento tecnologico di apposizione

Quale strumento tecnologico viene utilizzato per generare la firma elettronica.

Mezzo di attribuzione dell'elemento tecnologico a una persona

Come si lega l'elemento tecnologico alla persona fisica o giuridica.

Oggetto fisico per esercitare il dominio sulla firma

Come fa il titolare a firmare, avendo la certezza di poter essere l'unico a firmare.

Un soggetto fidato che garantisca l'identità del firmatario

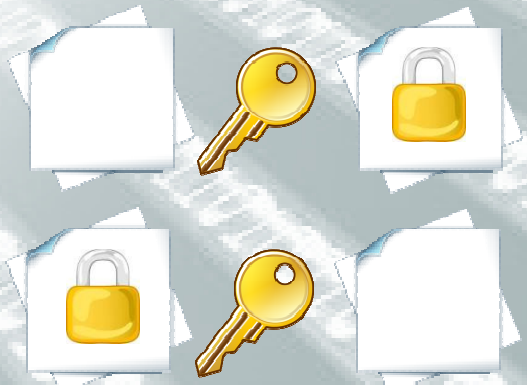
Chi garantisce l'associazione tra questi strumenti e la persona fisica.

La crittografia

La crittografia è la scienza che studia gli algoritmi matematici idonei a trasformare, in funzione di una chiave di cifratura, il contenuto di un messaggio in modo da renderne inintelligibile il messaggio.

La crittografia

La crittografia è la scienza che studia gli algoritmi matematici idonei a trasformare, in funzione di una chiave di cifratura, il contenuto di un messaggio in modo da renderne inintelligibile il messaggio.



Nella crittografia simmetrica le operazioni di cifratura e di decifratura richiedono la conoscenza di un'unica chiave.

La crittografia

La crittografia è la scienza che studia gli algoritmi matematici idonei a trasformare, in funzione di una chiave di cifratura, il contenuto di un messaggio in modo da renderne inintelligibile il messaggio.

Nella crittografia asimmetrica le operazioni di cifratura e di decifratura richiedono due chiavi distinte.

La crittografia a chiavi asimmetriche

La chiave di decifratura (o chiave privata) deve essere mantenuta segreta dal titolare, mentre la corrispondente chiave di cifratura (o chiave pubblica) è resa pubblica.

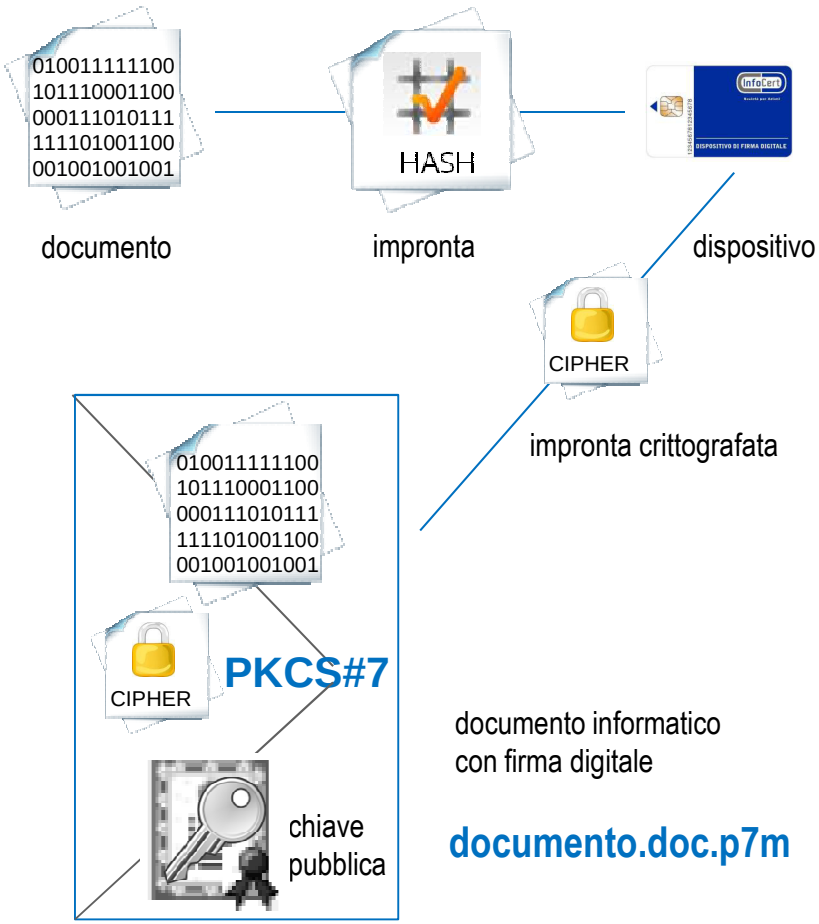
La lunghezza delle chiavi è di 1024 bit.

È *impossibile* risalire alla chiave privata partendo dalla chiave pubblica

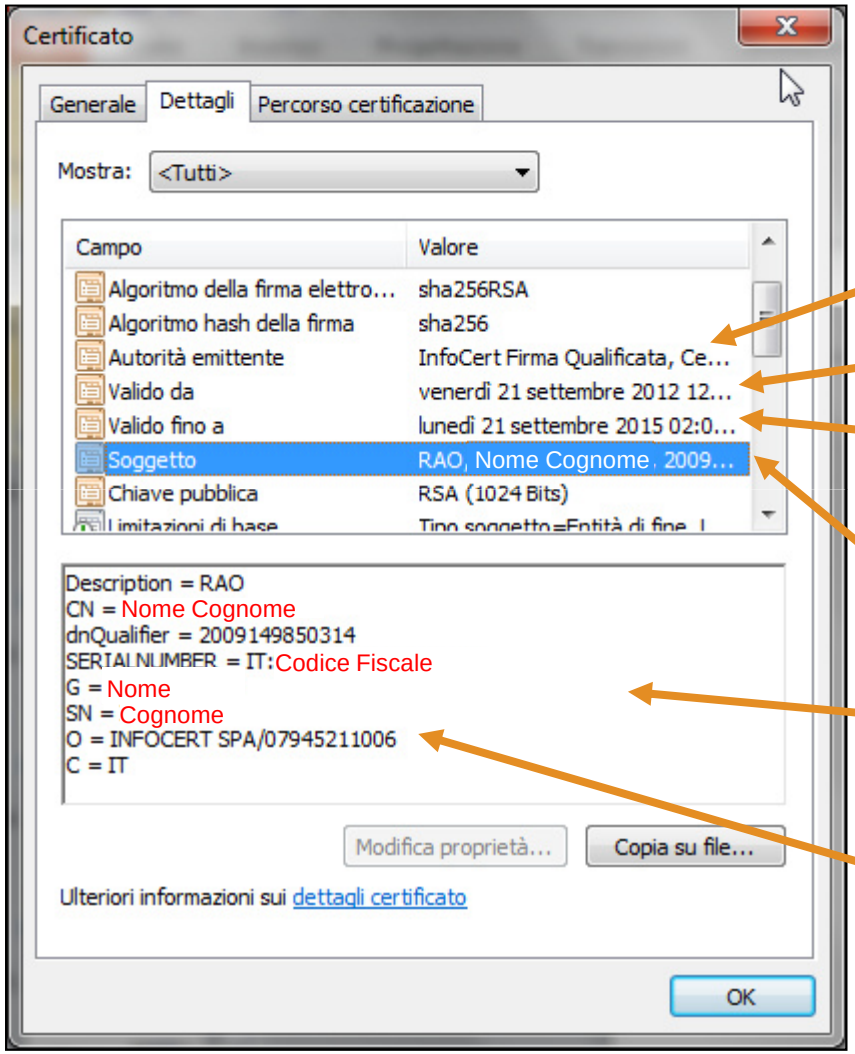
Le firma digitale

E’ una delle possibili applicazioni della crittografia a chiavi asimmetriche.

Il meccanismo consente di garantire al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, di rendere rispettivamente manifesta e di verificare l’autenticità e l'integrità di un documento informatico o di un insieme di documenti informatici.



Il certificato



Certification Authority

Data e ora di emissione

Data e ora di scadenza

Dati identificativi del soggetto e dettaglio

È possibile indicare l'organizzazione di appartenenza del titolare

Il certificato

Certificato di Sottoscrizione

Permette di apporre una firma digitale attribuendo valore legale al documento. E' generato seguendo indicazioni e standard normati.

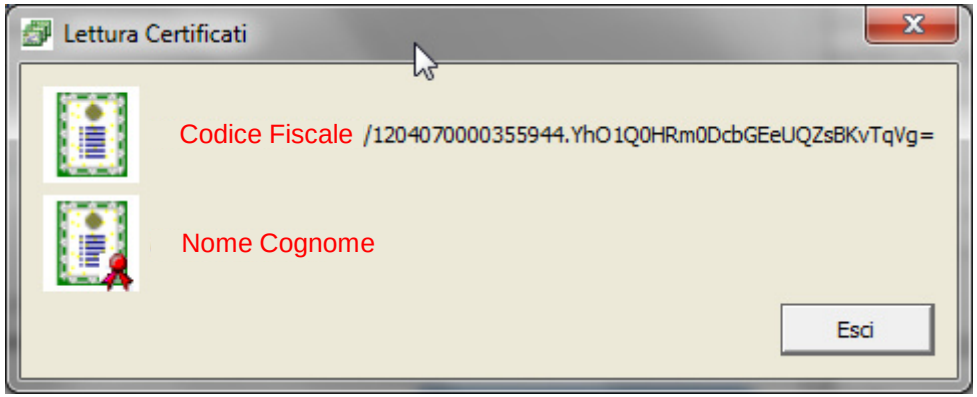
Certificato di Sottoscrizione con Ruolo

Permette di apporre una firma digitale attribuendo valore legale al documento. E' generato seguendo indicazioni e standard normati. Indica funzioni, titoli o abilitazioni professionali e poteri di rappresentanza del titolare.

Certificato di Autenticazione

Permette di autenticarsi a siti web e di firmare messaggi di posta elettronica.

Non è standardizzato.



Certificato di Autenticazione CNS

Permette di autenticarsi a siti web e di Firmare messaggi di posta elettronica.

Rilasciato dalla PA, è generato seguendo indicazioni e standard normati.

I dispositivi sicuri di firma

- ✓ supportano i certificati
- ✓ eseguono operazioni crittografiche al loro interno
- ✓ sono dotati di certificazione di sicurezza
- ✓ sono protetti da codici PIN

Il Certificatore

chi è

- Deve essere in possesso dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di direzione e controllo delle banche. Tali requisiti si estendono anche ai legali rappresentanti.
- La forma giuridica prevista è quella di società di capitali ed il capitale sociale deve essere pari o superiore a 6,5 milioni di €.
- Se non rilascia certificati qualificati, non deve richiedere autorizzazione preventiva.
- Se rilascia certificati qualificati, deve comunicare preventivamente all'Agenzia per l'Italia Digitale la sussistenza dei requisiti di onorabilità, nonché requisiti di:
  - affidabilità tecnica, organizzativa ed economica;
  - competenza del personale;
  - procedure di gestione;
  - sicurezza e anticontraffazione dei certificati.
- Deve accreditarsi presso AID iscrivendosi in un apposito albo: InfoCert è iscritta dal 19 luglio 2007. (http://www.digitpa.gov.it/firma-digitale/certificatori-accreditati/certificatori-attivi).

Il Certificatore

cosa fa

PROVVEDE ALL'IDENTIFICAZIONE DELLA PERSONA CHE RICHIEDE IL CERTIFICATO

- Direttamente o attraverso strutture collegate, si accerta delle generalità del richiedente il certificato.

RILASCIA IL CERTIFICATO

- Direttamente o attraverso strutture collegate, genera il certificato e lo mette a disposizione del titolare.

INFORMA I TITOLARI

- Rende disponibile e mantiene aggiornata la documentazione on-line per i titolari.

PROVVEDE ALLA TEMPESTIVA REVOCA E SOSPENSIONE DEL CERTIFICATO, SE RICHIESTO O NECESSARIO

- Mette a disposizione del Titolare o del Terzo Interessato gli strumenti per revocare/sospendere il certficato.

ASSICURA LA PRECISA DETERMINAZIONE DI DATA E ORA DI RILASCIO, REVOCA E SOSPENSIONE

- Garantisce la precisa rendicontazione temporale delle operazioni svolte.

REGISTRA TUTTE LE INFORMAZIONI RELATIVE AL CERTIFICATO PER 20 ANNI

- Mantiene la memoria di tutte le operazioni inerenti la vita del certificato.

Il Certificatore

cosa fa

PROVVEDE ALL'IDENTIFICAZIONE DELLA PERSONA CHE RICHIEDE IL CERTIFICATO

- Direttamente o attraverso strutture collegate, si accerta delle generalità del richiedente il certificato.

RILASCIA IL CERTIFICATO

- Direttamente o attraverso strutture collegate, genera il certificato e lo mette a disposizione del titolare

INFORMA I TITOLAR

- Rende disponibile

PROVVEDE ALLA TE ... **ARIO**

- Mette a disposizi

ASSICURA LA PREC

- Garantisce la pre

REGISTRA TUTTE LE

- Mantiene la mem

D.Lgs 82/2005 Codice dell'Amministrazione Digitale

Articolo 32. Obblighi del titolare e del certificatore

3. Il certificatore che rilascia, ai sensi dell' articolo 19, certificati qualificati deve inoltre:

a) provvedere con **certezza alla identificazione** della persona che fa richiesta della certificazione;

... omissis ...

4. Il certificatore è **responsabile dell'identificazione** del soggetto che richiede il certificato qualificato di firma **anche se tale attività è delegata a terzi;**

5. Il certificatore raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196 . I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono;

Il Certificatore

cosa fa

PROVVEDE ALL'IDENTIFICAZIONE DELLA PERSONA CHE RICHIEDE IL CERTIFICATO

- Direttamente o attraverso strutture collegate, si accerta delle generalità del richiedente il certificato.

RILASCIA IL CERTIFICATO

- Direttamente o attraverso strutture collegate, genera il certificato e lo mette a disposizione del titolare.

INFORMA I TITOLAR

- Rende disponibile

PROVVEDE ALLA TE

- Mette a disposizi

ASSICURA LA PREC

- Garantisce la pre

REGISTRA TUTTE LE

- Mantiene la mem

D.Lgs 82/2005 Codice dell'Amministrazione Digitale

Articolo 32. Obblighi del titolare e del certificatore

3. Il certificatore che rilascia, ai sensi dell' articolo 19, certificati qualificati deve inoltre:

a) … omissis …

b) rilasciare e rendere pubblico il certificato elettronico nei modi o nei casi stabiliti dalle regole tecniche di cui all' articolo 71, nel rispetto del decreto legislativo 30 giugno 2003, n. 196 , e successive modificazioni;

c) specificare, nel certificato qualificato **su richiesta** dell'istante, e **con il consenso del terzo interessato**, i **poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite**, previa verifica della documentazione presentata dal richiedente che attesta la sussistenza degli stessi;

Il Certificatore

cosa fa

PROVVEDE ALL'IDENTIFICAZIONE DELLA PERSONA CHE RICHIEDE IL CERTIFICATO

- Direttamente o attraverso strutture collegate, si accerta delle generalità del richiedente il certificato.

RILASCIA IL CERTIFICATO

- Direttamente o attraverso strutture collegate, genera il certificato e lo mette a disposizione del titolare.

INFORMA I TITOLARI

- Rende disponibile e mantiene aggiornata la documentazione on-line per i titolari.

PROVVEDE ALLA TE

- Mette a disposizi

ASSICURA LA PREC

- Garantisce la pre

REGISTRA TUTTE LE

- Mantiene la mem

D.Lgs 82/2005 Codice dell'Amministrazione Digitale

Articolo 32. Obblighi del titolare e del certificatore

3. Il certificatore che rilascia, ai sensi dell' articolo 19, certificati qualificati deve inoltre:

… omissis …

e) **informare** i richiedenti in modo compiuto e chiaro, **sulla procedura di certificazione** e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;

… omissis …

l) predisporre su **mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio** di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette **informazioni**, che possono essere trasmesse elettronicamente, devono essere **scritte in linguaggio chiaro ed essere fornite prima dell'accordo** tra il richiedente il servizio ed il certificatore;

Il Certificatore

D.Lgs 82/2005 Codice dell'Amministrazione Digitale

Articolo 32. Obblighi del titolare e del certificatore

3. Il certificatore che rilascia, ai sensi dell' articolo 19, certificati qualificati deve inoltre:

… omissis …

g) procedere alla **tempestiva pubblicazione della revoca e della sospensione** del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri del titolare medesimo, di perdita del possesso o della compromissione del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni, secondo quanto previsto dalle regole tecniche di cui all' articolo 71;

h) garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo nonché garantire il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;

PROVVEDE ALLA TEMPESTIVA REVOCA E SOSPENSIONE DEL CERTIFICATO, SE RICHIESTO O NECESSARIO

- Mette a disposizione del Titolare o del Terzo Interessato gli strumenti per revocare/sospendere il certficato.

ASSICURA LA PRECISA DETERMINAZIONE DI DATA E ORA DI RILASCIO, REVOCA E SOSPENSIONE

- Garantisce la precisa rendicontazione temporale delle operazioni svolte.

REGISTRA TUTTE LE INFORMAZIONI RELATIVE AL CERTIFICATO PER 20 ANNI

- Mantiene la memoria di tutte le operazioni inerenti la vita del certificato.

Il Certificatore

cosa fa

PROVVEDE ALL'IDENTIFICAZIONE DELLA PERSONA CHE RICHIEDE IL CERTIFICATO

- Direttamente o attraverso strutture collegate, si accerta delle generalità del richiedente il certificato.

RILASCIA IL CERTIFICAT

- Direttamente o attrave

INFORMA I TITOLARI

- Rende disponibile e m

PROVVEDE ALLA TEMPE

- Mette a disposizione del Titolare o del Terzo Interessato gli strumenti per revocare/sospendere il certficato.

D.Lgs 82/2005 Codice dell'Amministrazione Digitale
Articolo 32. Obblighi del titolare e del certificatore
3. Il certificatore che rilascia, ai sensi dell' articolo 19, certificati qualificati deve inoltre:
… omissis …
i) assicurare la **precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione** dei certificati elettronici;

ASSICURA LA PRECISA DETERMINAZIONE DI DATA E ORA DI RILASCIO, REVOCA E SOSPENSIONE

- Garantisce la precisa rendicontazione temporale delle operazioni svolte.

REGISTRA TUTTE LE INFORMAZIONI RELATIVE AL CERTIFICATO PER 20 ANNI

- Mantiene la memoria di tutte le operazioni inerenti la vita del certificato.

Il Certificatore

cosa fa

PROVVEDE ALL'IDENTIFICAZIONE DELLA PERSONA CHE RICHIEDE IL CERTIFICATO

- Direttamente o attraverso strutture collegate, si accerta delle generalità del richiedente il certificato.

RILASCIA IL CERTIFICATO

- Direttamente o attraverso strutture collegate, genera il certificato e lo mette a disposizione del titolare.

INFORMA I TITOLARI

- Rende disponibile e m

PROVVEDE ALLA TEMPE

- Mette a disposizione d

ASSICURA LA PRECISA

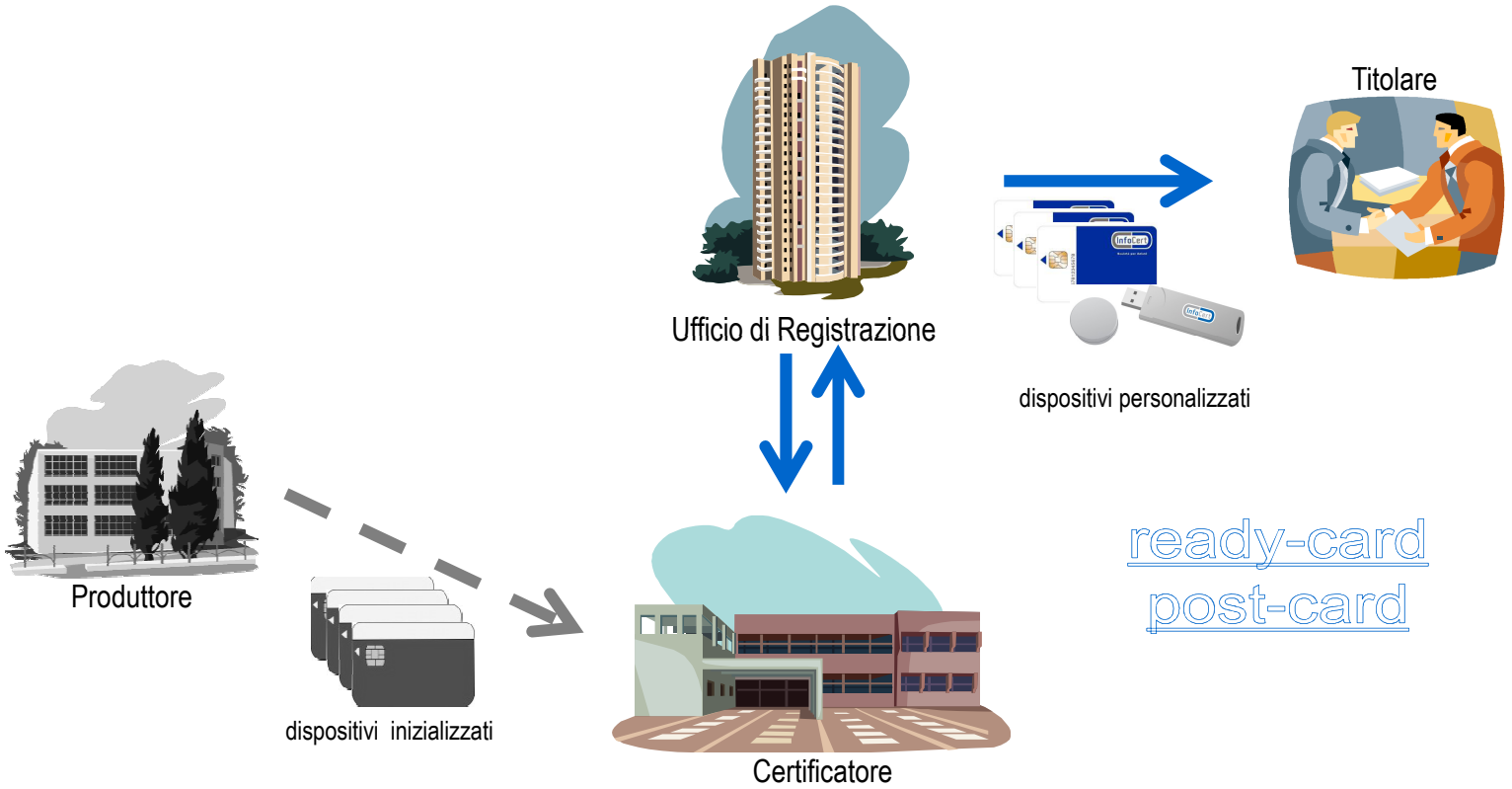
- Garantisce la precisa rendicontazione temporale delle operazioni svolte.

D.Lgs 82/2005 Codice dell'Amministrazione Digitale
Articolo 32. Obblighi del titolare e del certificatore
3. Il certificatore che rilascia, ai sensi dell' articolo 19, certificati qualificati deve inoltre:
… omissis …
j) tenere **registrazione**, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno **per venti anni** anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;

REGISTRA TUTTE LE INFORMAZIONI RELATIVE AL CERTIFICATO PER 20 ANNI

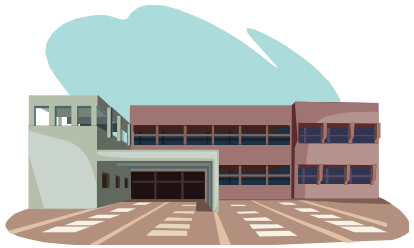
- Mantiene la memoria di tutte le operazioni inerenti la vita del certificato.

Chi fa che cosa



Chi fa che cosa

il Certificatore



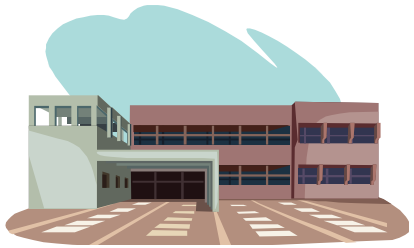
- Emette i certificati qualificati, su richiesta li pubblica in un apposito registro, ne consente il rinnovo, la revoca o la sospensione, operando in conformità alle Regole Tecniche e secondo quanto prescritto dal C.A.D.

- Pubblica il **Manuale Operativo**, un documento digitale che contiene:
  - ✓ la descrizione delle procedure adottate dal Certificatore per la fornitura dei servizi di certificazione digitale e di validazione temporale;
  - ✓ la descrizione delle misure di sicurezza adottate dal Certificatore per garantire
  - ✓ le regole generali per l'emissione e l'utilizzo dei certificati e delle chiavi di sottoscrizione.

  Il Manuale Operativo è parte integrante del contratto di erogazione del servizio.

Chi fa che cosa

il Certificatore



- Deve garantire:
  - ✓ l'unicità della chiave pubblica nel proprio dominio;
  - ✓ la generazione di un codice identificativo univoco del certificato rilasciato (IUT) al momento della registrazione dei dati del titolare;
  - ✓ la pubblicazione del certificato su richiesta del titolare;
  - ✓ l'indicazione della sussistenza di poteri o titoli, con il consenso della Terza Parte Interessata, all'interno del certificato.

- Poiché garantisce l'intero processo, viene anche definito **Terza Parte Fidata**.

Chi fa che cosa

l'Ufficio di Registrazione

- Svolge la sua attività a seguito della sottoscrizione di una **Convenzione** con InfoCert., un accordo contrattuale che regola i rapporti con l'Ente Certificatore indicando i reciproci impegni nell'esecuzione delle attività.

- Rappresenta l'Ente Certificatore e coopera nell'emissione di un certificato attraverso:
  - ✓ la verifica degli aspetti formali;
  - ✓ l'identificazione del titolare;
  - ✓ l'avvio della procedura di emissione dei certificati;
  - ✓ la distribuzione dei dispositivi di firma.

- Supporta l'Ente Certificatore nelle fasi di revoca, sospensione e rinnovo.

Chi fa che cosa

l'Ufficio di Registrazione

- Nell'ambito di un Ufficio di Registrazione operano:

  ✓ il **RAO** (Addetto all'Ufficio di Registrazione)

  identifica il titolare e le condizioni di sussitenza di un titolo/ ruolo;
  registra i dati del titolare sull'applicativo per il rilascio dei certificati;
  richiede l'emissione dei certificati su Business Key o smart card;
  consegna al titolare il dispositivo, la cartellina contenente le condizioni generali di contratto e i codici di sicurezza.

  ✓ l'**IR** (Incaricato alla Registrazione)

  identifica il titolare e le condizioni di esistenza di un titolo/ruolo;
  registra i dati del titolare su sito o su modulo cartaceo;
  consegna al titolare la cartellina contenente le condizioni generali di contratto e i codici di sicurezza;
  consegna al titolare il dispositivo, se incaricato dal RAO.

Chi fa che cosa

l'Ufficio di Registrazione

- Deve garantire:
  - ✓ la verifica dell'identità del titolare attraverso l'esibizione di un documento di identità in corso di validità;
  - ✓ l'informazione del Titolare sugli obblighi di protezione della segretezza della chiave privata;
  - ✓ la custodia accurata del proprio dispositivo di firma contenete il certificato RAO, del PIN, della cartellina di revoca e delle credenziali di accesso all'applicativo per il rilascio dei certificati.

Chi fa che cosa

l'Ufficio di Registrazione

- Deve garantire:
  - ✓ la raccolta delle Richieste di Registrazione e Certificazione debitamente compilate e firmate dal titolare;
  - ✓ l'apposizione della sua firma su ciascuna Richiesta;
  - ✓ la consegna di una copia della Richiesta al titolare quale ricevuta delle attività di registrazione svolte;
  - ✓ la spedizione **mensile** delle Richieste all'Ente Certificatore al seguente indirizzo:

InfoCert
C.so Stati Uniti, 14bis
35127 Padova
Ufficio Archiviazione Digitale

Chi fa che cosa

il Titolare

- E’ una persona fisica, maggiorenne, dotata di codice fiscale o identificativo equivalente (https://en.wikipedia.org/wiki/National_identification_number).
- E’ identificato come il possessore della chiave privata corrispondente alla chiave pubblica contenuta nel certificato.
- Per questo motivo, la firma digitale generata con la chiave privata della coppia è attribuita al titolare.
- Al termine del processo di registrazione e certificazione, riceve:

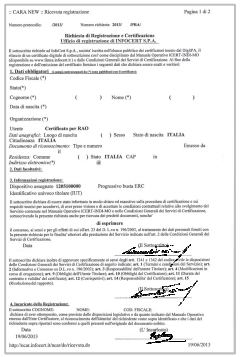
Chi fa che cosa

il Titolare

- E’ una persona fisica, maggiorenne, dotata di codice fiscale o identificativo equivalente (https://en.wikipedia.org/wiki/National_identification_number).
- E’ identificato come il possessore della chiave privata corrispondente alla chiave pubblica contenuta nel certificato.
- Per questo motivo, la firma digitale generata con la chiave privata della coppia è attribuita al titolare.
- Al termine del processo di registrazione e certificazione, riceve:

dispositivo di firma

ricevuta



cartellina con contratto e codici di sicurezza

manuale operativo
(riferimento web)

Chi fa che cosa

il Titolare

- Il Titolare **deve**:
  - ✓ custodire con la massima cura la chiave privata (ovvero il dispositivo di firma);
  - ✓ custodire con la massima cura il PIN;
  - ✓ conservare il codice di emergenza (ERC);
  - ✓ utilizzare in esclusiva il dispositivo di firma.

Chi fa che cosa

altri

- Il Produttore di dispositivi crittografici è tenuto a garantire i seguenti aspetti del processo di certificazione:
  - ✓ produzione dei chip secondo gli standard previsti dalla normativa;
  - ✓ conservazione dei chip e embedding;
  - ✓ inizializzazione elettrica;
  - ✓ procedure di invio dei lotti di smart card o token USB inizializzati al Certificatore inclusa l'assegnazione del PIN di trasporto.

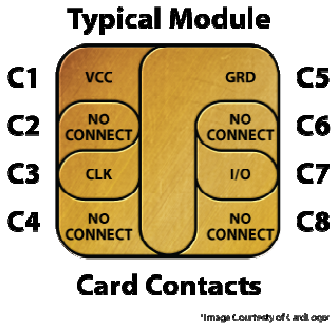


*Image courtesy of [illegible]

Chi fa che cosa

altri

- Il **Terzo Interessato** è la persona, fisica o giuridica, che acconsente al rilascio di certificati qualificati nei quali sia riportata l'appartenenza ad un'organizzazione ovvero eventuali poteri di rappresentanza o titoli e cariche rivestite.
  Può/deve richiedere la revoca o la sospensione del certificato qualora i requisiti in base ai quali il certificato è stato rilasciato siano mutati.

- L'**Utente generico** è chiunque entri in possesso di un documento firmato digitalmente ed assume l'onere di verificare le firme apposte.

La procedura di rilascio

Cose da fare per rilasciare un certificato

- prenotazione, opzionale (https://ncar.infocert.it/pcarweb/default.do)
- identificazione del titolare
- registrazione dei dati
- emissione dei certificati
- inizializzazione del dispositivo di firma

La procedura di rilascio

identificazione

Cose da fare per rilasciare un certificato

La richiesta di rilascio di un certificato implica la necessità di riconoscere il titolare. L'identificazione:

- è eseguita dal personale dell'Ufficio di Registrazione;
- prevede la presenza fisica del Titolare (non è ammessa delega) e si basa sul controllo di un documento identità valido (art. 35 TU , D.P.R. 28/12/2000, n.445) ed eventualmente dell'attestazione del ruolo.

Codice Fiscale

documenti di identità

ecc., ….

La procedura di rilascio

registrazione

Cose da fare per rilasciare un certificato

I dati del Titolare sono registrati nel DB del Certificatore.

- Se la fase di registrazione è contestuale a quella di identificazione, emissione e consegna del dispositivo, si parla di registrazione ready-card
- Se le fasi di identificazione, registrazione, emissione e consegna del dispositivo sono separate tra loro, si parla di registrazione post-card
  In questo caso è possibile che intervengano le due figure cui è demandata l'attività di riconoscimento, RAO e IR.

La procedura di rilascio

emissione

Cose da fare per rilasciare un certificato

Il RAO richiede l'emissione del certificato.

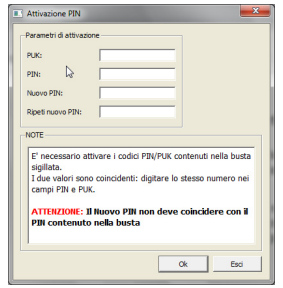
- All'interno del dispositivo di firma, in un'area protetta indenne alla formattazione, viene generata la coppia di chiavi asimmetriche.
- Il RAO, con la digitazione del PIN, sottoscrive la richiesta di emissione del certificato.
- Dopo gli opportuni controlli, InfoCert genera il certificato e ne permette il salvataggio sul dispositivo.
- Il certificato emesso è inserito nel Registro dei Certificati ma viene reso pubblico solo su esplicita richiesta del Titolare.

La procedura di rilascio

Cose da fare per rilasciare un certificato

Il Titolare attiva il suo dispositivo di firma personalizzando il PIN.

- L'attivazione del PIN è propedeutica all'utilizzo del dispositivo di firma.
- I codici richiesti per l'attivazione, PIN e PUK, sono contenuti nella cartellina ERC.
- Il Titolare modifica il PIN, il PUK rimane immodificato.
- Nella cartellina è contenuto un ulteriore codice di sicurezza, l'Emergency Request Code, necessario per la sospensione on-line del certificato.



La validità dei certificati

revoca - sospensione

- In condizioni standard il certificato digitale ha una validità di **3 anni**.
- La **revoca** o la **sospensione** modificano la validità del certificato anticipandola e ne comportano l'inserimento nella lista dei certificati revocati e sospesi o **CRL**.
- La revoca o la sospensione rendono le firme apposte dopo la pubblicazione della CRL non valide.
- La sospensione ha carattere di temporaneità, la revoca è un processo definitivo.

La validità dei certificati

revoca - sospensione

- La lista dei certificati revocati o sospesi ha una frequenza di emissione e pubblicazione che contempla:

  ✓ **l'emissione ordinaria**

  pubblicazione quotidiana, il tempo massimo di attesa è di 24 ore;

  ✓ **l'emissione straordinaria**

  pubblicazione immediata , il tempo massimo di attesa è di 1 ora.

Se è la chiave privata ad essere compromessa, allora la revoca/sospensione del certificato non possono che essere immediate

La validità dei certificati

revoca - sospensione

- La revoca o la sospensione dei certificati possono essere richiesti da:
  - ✓ **Titolare**
  - ✓ **Certificatore**
  - ✓ **Terzo Interessato**
- Le modalità e gli strumenti utilizzati per richiedere la revoca o la sospensione possono variare in funzione del richiedente.

Il Titolare

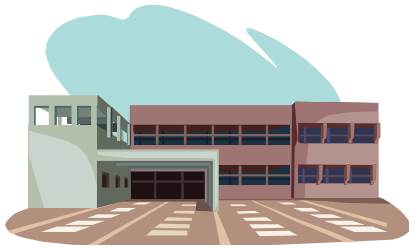
- ✓ può **richiedere la revoca** tramite l'Ufficio di Registrazione o direttamente al Certificatore inviando una lettera o un fax con allegata la fotocopia di un documento di identità;
- ✓ può **richiedere la sospensione** tramite il sito o il call center del Certificatore, ovvero tramite l'Ufficio di Registrazione o direttamente al Certificatore inviando una lettera o un fax con fotocopia del documento di identità.

La validità dei certificati

revoca - sospensione

- La revoca o la sospensione dei certificati possono essere richiesti da:
  - ✓ **Titolare**
  - ✓ **Certificatore**
  - ✓ **Terzo Interessato**
- Le modalità e gli strumenti utilizzati per richiedere la revoca o la sospensione possono variare in funzione del richiedente.

Il Certificatore



✓ **attiva la revoca** o **la sospensione** del certificato comunicando preventivamente al Titolare, salvo casi d'urgenza, l'intenzione di sospendere il certificato e fornendo il motivo della revoca o sospensione, la data di decorrenza e la data di termine della sospensione.

La validità dei certificati

revoca - sospensione

- La revoca o la sospensione dei certificati possono essere richiesti da:
  - ✓ **Titolare**
  - ✓ **Certificatore**
  - ✓ **Terzo Interessato**
- Le modalità e gli strumenti utilizzati per richiedere la revoca o la sospensione possono variare in funzione del richiedente.

Il Terzo Interessato

- ✓ può **richiedere la revoca** o **la sospensione** tramite l'Ufficio di Registrazione o direttamente al Certificatore, inviando il modulo disponibile sul sito
- ✓ modalità aggiuntive per la richiesta di sospensione da parte del Terzo Interessato potranno essere specificate negli eventuali accordi stipulati tra quest'ultimo ed il Certificatore.

La validità dei certificati

revoca

- La **revoca** di un certificato può essere richiesta a causa di:
  - ✓ chiave privata compromessa, ovvero smarrimento del dispositivo di firma, perdita della segretezza della chiave o del PIN
  - ✓ dispositivo di firma non funzionante
  - ✓ modifica dei dati del Titolare presenti nel certificato
  - ✓ disdetta
  - ✓ mancato rispetto del Manuale Operativo

La validità dei certificati

sospensione

- La **sospensione** di un certificato può essere richiesta a causa di:
  - ✓ necessità di interrompere la validetà del certificato
  - ✓ dubbi sulla validità del certificato
  - ✓ dubbi sull'opportunità di una richiesta di revoca
- Al termine del periodo di sospensione richiesto, la validità del certificato viene ripristinata automaticamente poiché il certificato è rimosso dalla lista di revoca e sospensione (CRL).
- Un certificato sospeso può essere revocato.
- Non è possibile anticipare il ripristino della validità di un certificato prima che termini il suo periodo di sospensione.

La validità dei certificati

rinnovo

- In condizioni standard il certificato digitale ha una validità di **3 anni**.
- La procedura di **rinnovo** del certificato permette di prorogare per ulteriori **3 anni** la validità del certificato purché venga eseguita prima della data di fine validità del certificato.
- Superata questa data, il rinnovo non è più consentito; il titolare deve chiedere l'emissione di un nuovo certificato.
- Al momento del rinnovo viene generata una nuova coppia di chiavi ed un nuovo certificato.
- I certificati scaduti restano archiviati per 20 anni.

La validità dei certificati

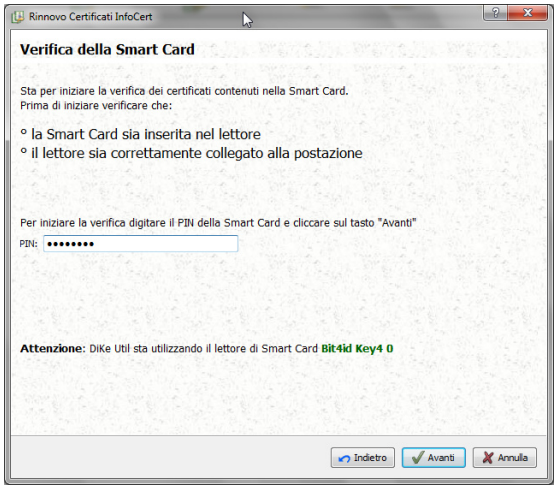
rinnovo

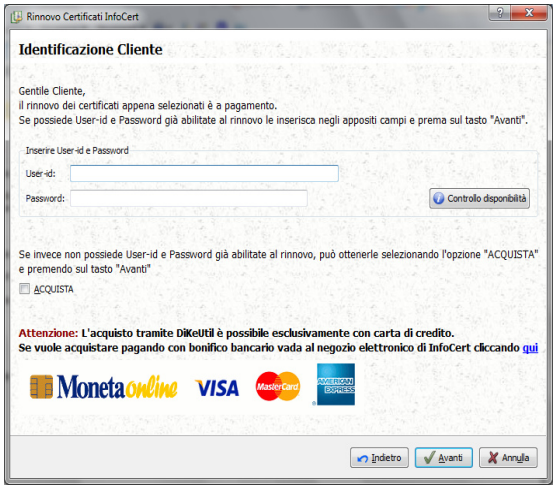
- Se la procedura di rinnovo è eseguita dal Titolare, questi dovrà:
  - ✓ registrarsi sul negozio elettronico InfoCert e recuperare le credenziali di accesso;
  - ✓ acquistare i certificati effettuando il pagamento con carta di credito, bonifico o tramite un punto Sisal Pay;
  - ✓ i certificati acquistati vengono accreditati sulle credenziali del negozio;
  - ✓ procedere con il rinnovo dei certificati utilizzando **Dike Util**; il software richiederà l'inserimento del PIN del dispositivo e delle credenziali di accesso fornite dal negozio elettronico.

La validità dei certificati

rinnovo

- Se la procedura di rinnovo è eseguita dal RAO, questi dovrà:
  - ✓ procedere con il rinnovo dei certificati utilizzando **Dike Util**; il software richiederà l'inserimento del PIN del dispositivo e delle credenziali di accesso del RAO;
  - ✓ i certificati acquistati vengono addebitati all'Ufficio di Registrazione.





Orari di disponibilità dei servizi

Servizio	Orario
Accesso all'archivio pubblico dei certificati e alla CRL	24hx7gg
Revoca e sospensione dei certificati	24hx7gg
Registrazione dati, generazione certificati, pubblicazione	dal lunedì al venerdì 09:00 – 17:00 sabato 09:00 – 13:00 esclusi i festivi
Richiesta e/o verifica di marca temporale	24hx7gg

Numeri utili

Call Center per i RAO

800 777 578

Call Center per gli utenti finali

199 500 130

Per maggiori informazioni:

www.infocert.it