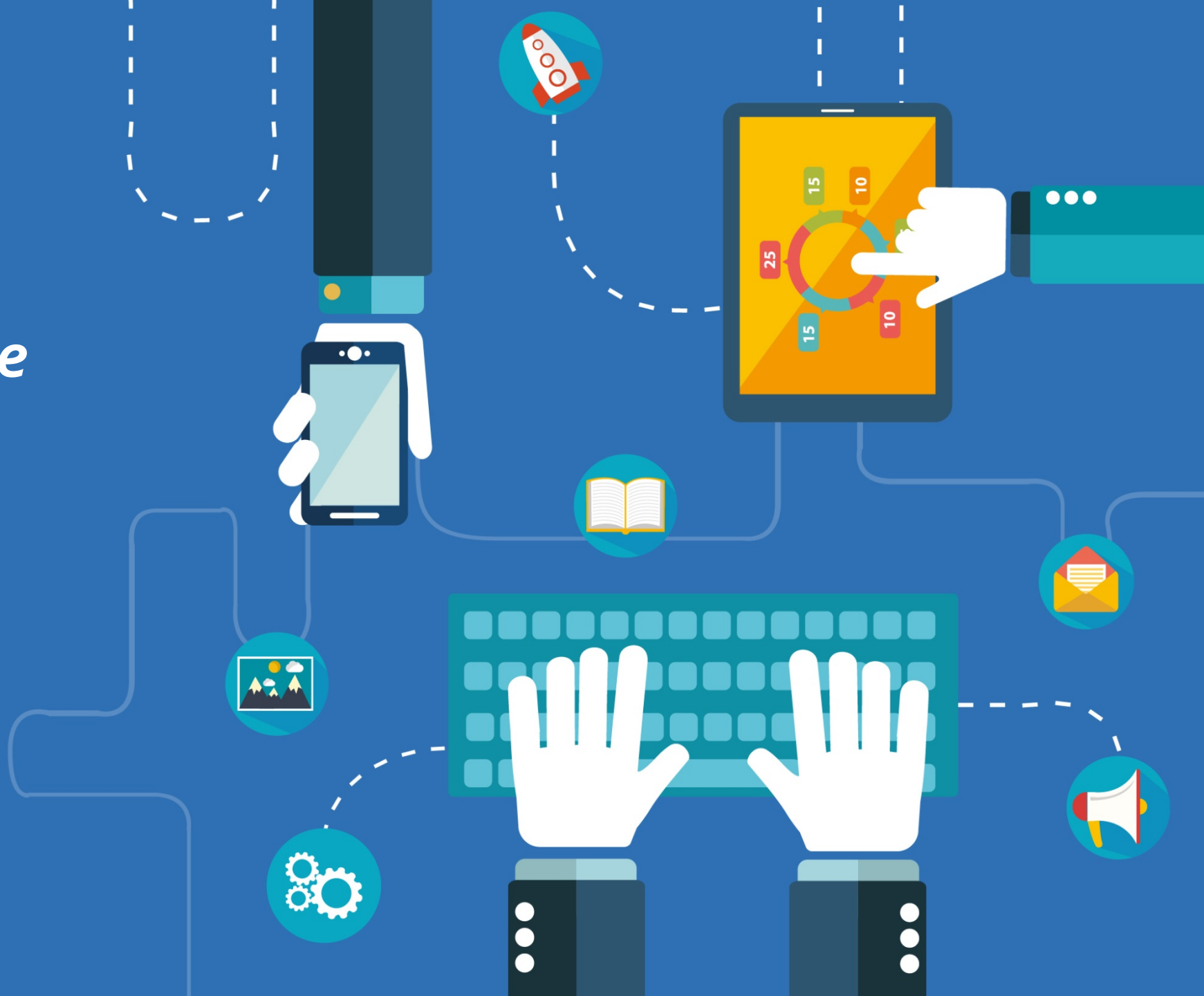
Titolo presentazione

Data gg/mm/aaaa

Autore



Agenda

RAO

Addetti agli Uffici di Registrazione

1

Conoscenze di base

 *Crittografia*

 *Firma digitale*

 *Certificato e certificatore*

 *Organizzazione e procedura*

 *Manuale operativo*

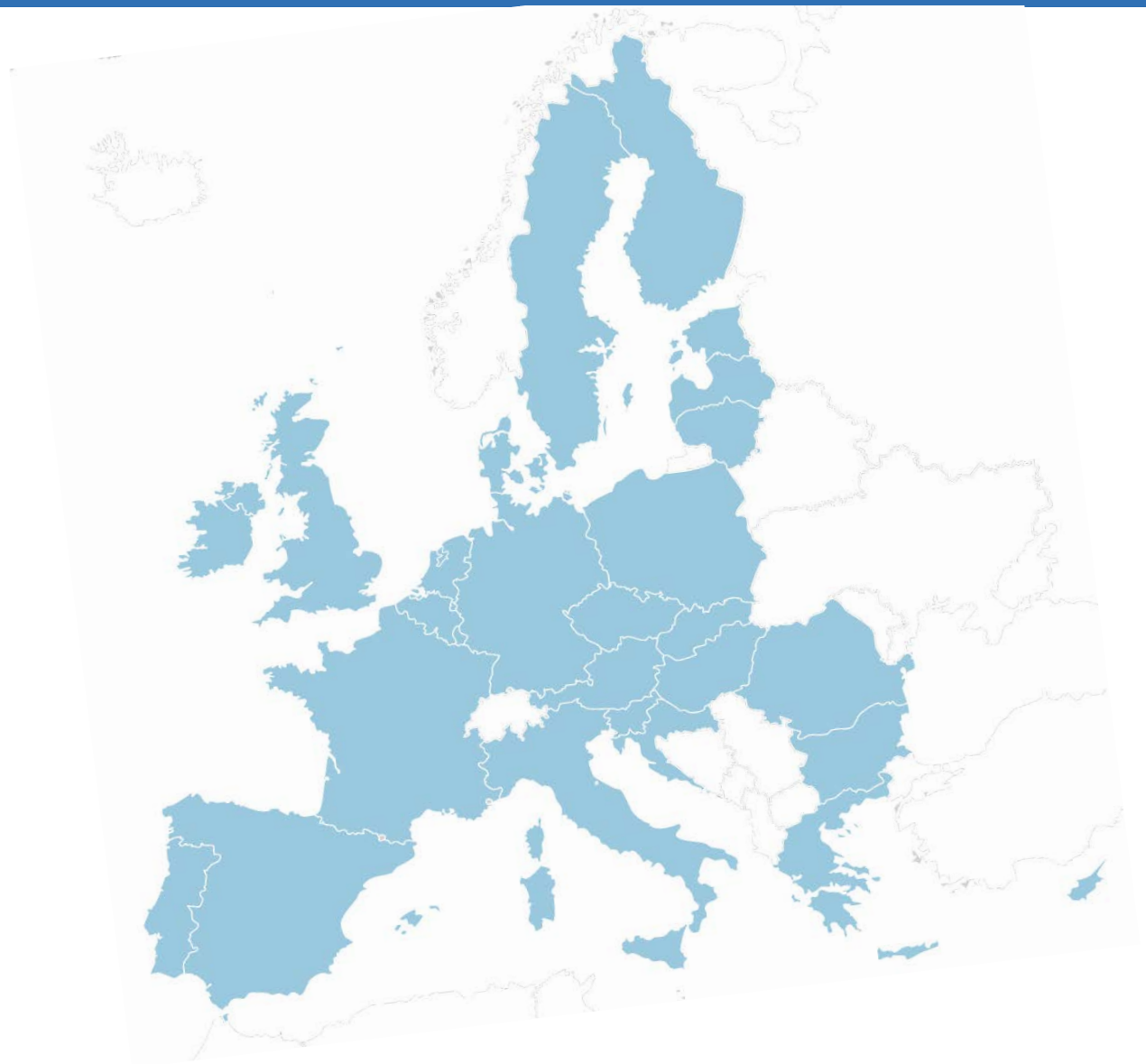
2

Operatività

 *Registrazione e emissione*

 *Attivazione dispositivo di firma*

Contesto normativo



<u>Legale</u>

REGOLAMENTO (EU) N. 910/2014: electronic identification and trust services for electronic transactions nel mercato internazionale (**eIDAS**).

<u>Tecnica</u>

a) Specifiche tecniche rispetto alle **trusted lists** (*1505/2015*);
b) Specifiche tecniche rispetto alle firme elettroniche avanzate e ai sigilli avanzati che gli organismi del settore pubblico devono riconoscere.

<u>Legale</u>

D.LGS. N. 82/2005: Codice dell'Amministrazione Digitale **(CAD)**.

<u>Tecnica</u>

a) Regole tecniche in materia di **generazione**, apposizione e verifica delle firme elettroniche avanzate, qualificate e **digitali** (*DPCM 22/02/2013*);
b) Regole tecniche in materia di **formazione**, trasmissione, copia, duplicazione, riproduzione e **validazione temporale** dei documenti informatici nonché di formazione e conservazione dei documenti informatici (DPCM 13/11/2014).

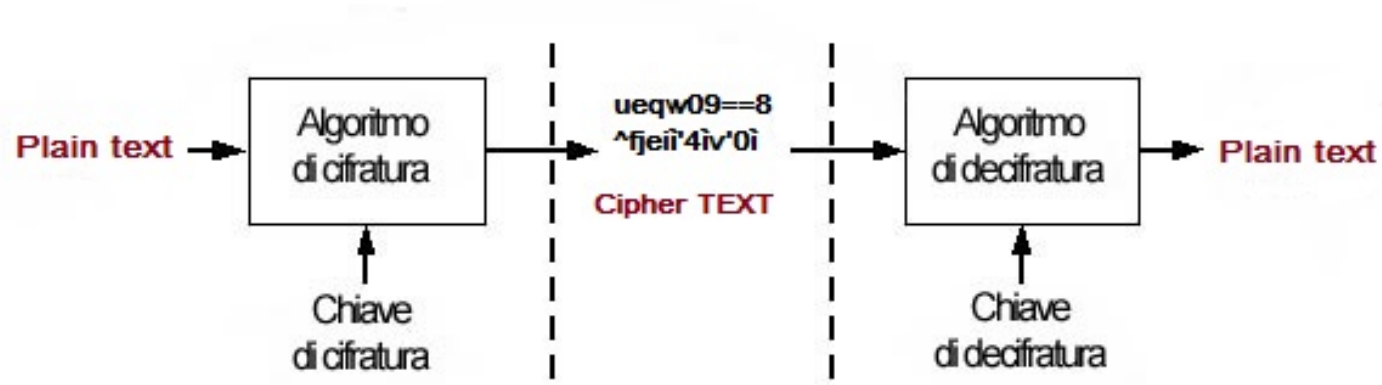
Crittografia

Si parla di testo in chiaro (plain-text) riferendosi al messaggio originale.

Il testo in chiaro viene crittografato mediante l'uso di una apposita chiave, a questo punto il messaggio prende il nome di testo cifrato (cipher-text).

Se la stessa chiave usata per la cifratura viene usata per la decifratura del messaggio e si parla di crittografia simmetrica.

Quando invece la chiave usata per la decifrazione è diversa da quella usata per la cifratura si parla di crittografia asimmetrica (o a chiave pubblica).



Cifratura asimmetrica: RSA

- Come funziona: esistono 2 chiavi per un unico soggetto: pubblica e privata (o segreta)
  - chiave pubblica ->informazione da diffondere
  - chiave segreta -> segreto da custodire

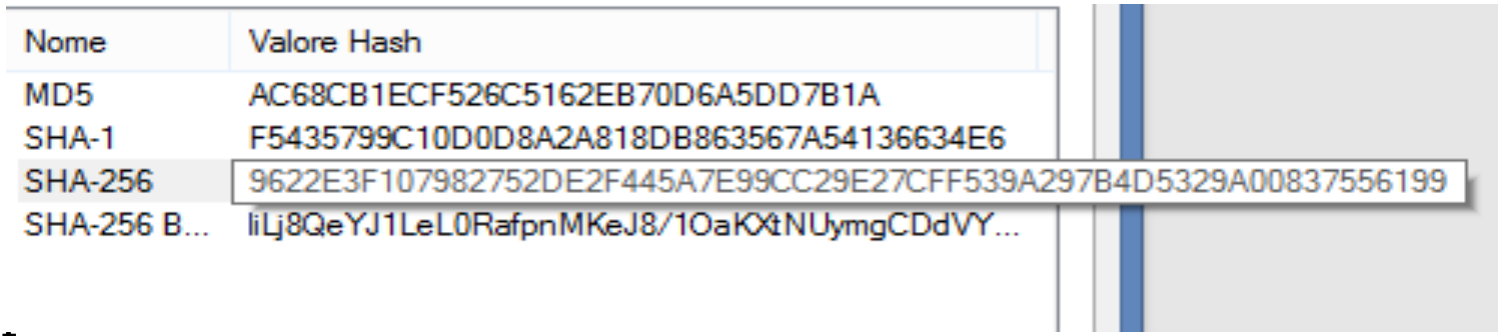
- La sicurezza è data dalla difficoltà di fattorizzare un numero intero (ALGORITMO ROBUSTO). La chiave pubblica è un numero P ottenuto moltiplicando due numeri primi molto grandi che restano segreti (SEGRETO)

  - chiave pubblica -> serve per cifrare (integrità e riservatezza),
  - chiave segreta -> per firmare (non ripudio)

Violare il sistema RSA è difficile quanto la fattorizzazione dei numeri primi
Chiave 512->poche ore
Chiave 1024->un anno

Algoritmi di hash

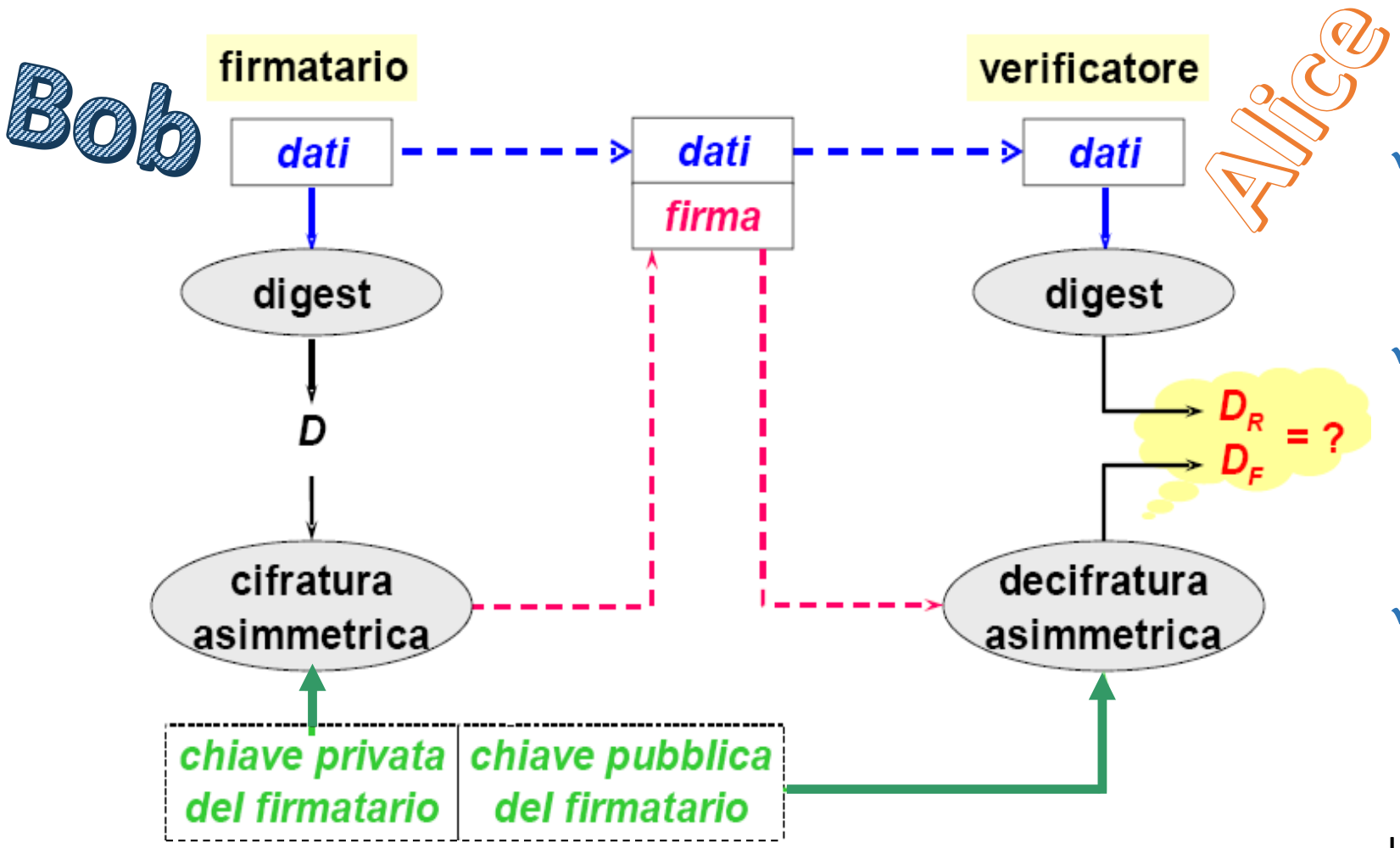
- Funzione di hash:
  - calcola un valore di lunghezza fissa e ridotta (impronta) a partire da un oggetto di dimensioni arbitrarie
  - funzione unidirezionale
  - documenti diversi => impronte diverse (bassa probabilità di collisione)
- Algoritmi:
  - Sha-1, ripemd-160, md5, sha-256



Nome	Valore Hash
MD5	AC68CB1ECF526C5162EB70D6A5DD7B1A
SHA-1	F5435799C10D0D8A2A818DB863567A54136634E6
SHA-256	9622E3F107982752DE2F445A7E99CC29E27CFF539A297B4D5329A00837556199
SHA-256 B...	liLj8QeYJ1LeL0RafpnMKeJ8/1OaKXtNUymgCDdVY...

Usati come sinonimi: impronta o digest

Firma elettronica



- ✓ Il mittente usa la chiave privata per cifrare
- ✓ Non viene cifrato l'intero messaggio, ma la sua impronta
- ✓ Con la chiave pubblica si decifra e chi decifra ha la certezza di chi ha cifrato

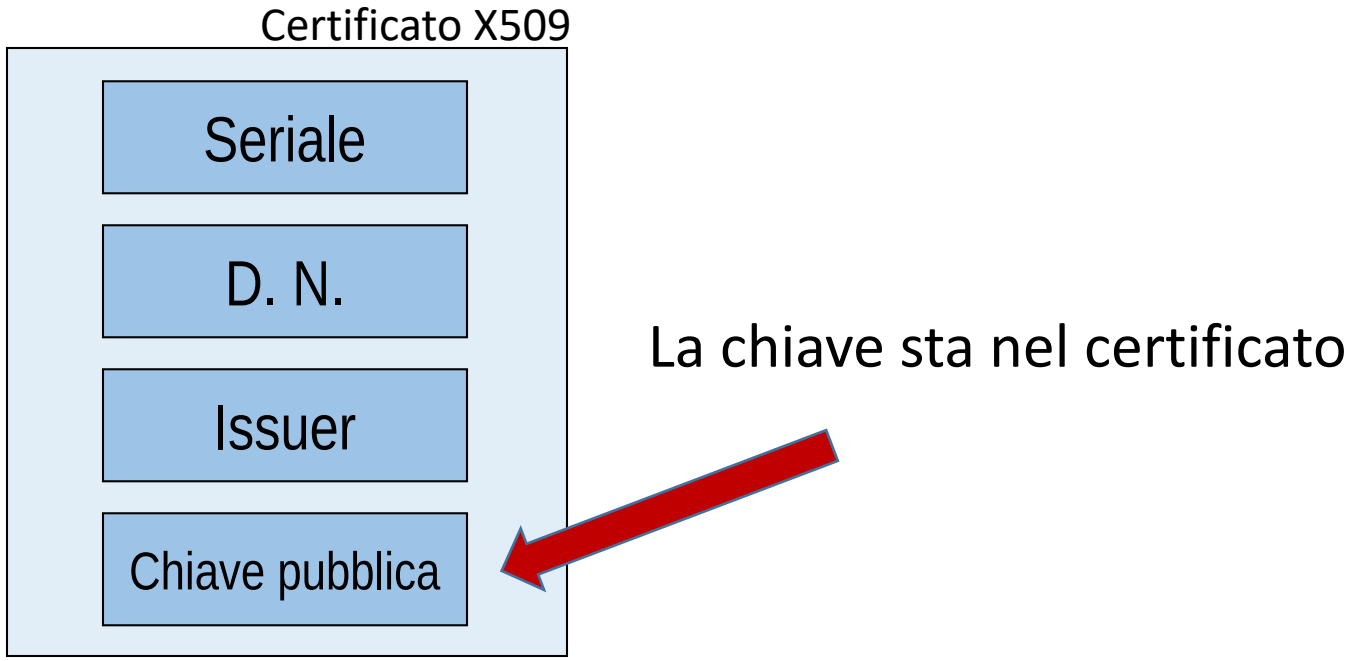
In questo modo ottengo il non ripudio

Certificato digitale

Come ottengo la chiave pubblica di Bob?

Come faccio a sapere che questa chiave pubblica appartiene effettivamente a Bob?

Come faccio a sapere se la chiave pubblica di Bob è tuttora valida?

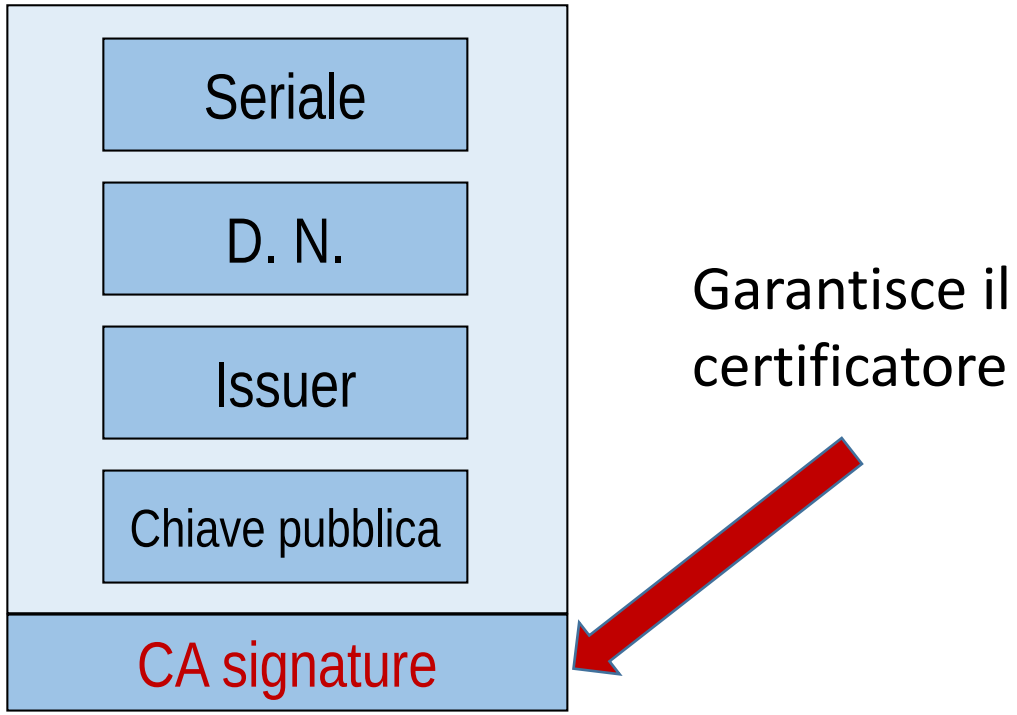


Certificato digitale

Come ottengo la chiave pubblica di Bob?

Come faccio a sapere che questa chiave pubblica appartiene effettivamente a Bob?

Come faccio a sapere se la chiave pubblica di Bob è tuttora valida?



Garantisce il certificatore

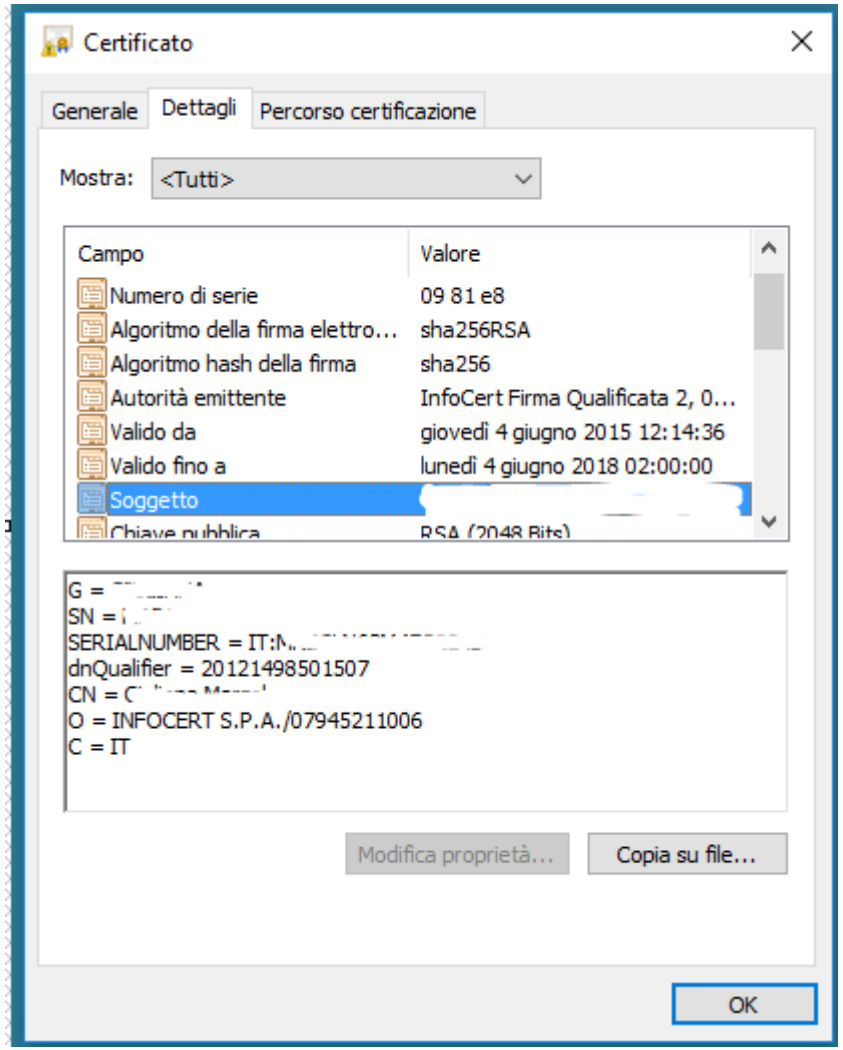
Certificato digitale

E' l'associazione tra un'identità e una coppia di chiavi pubblica/privata in possesso di chi detiene tale identità. La CA viene consultata per la verifica e attestazione di detta identità.

Informazioni principali

Subject/Soggetto	individuo o altra entità che viene identificata dal certificato.
Public Key/Chiave Pubblica	la chiave pubblica corrispondente a quella privata che possiede il soggetto
Issuer/Emittente	l'emittente (CA) di fiducia che ha generato e firmato il certificato;
Serial Number/Numero di serie	identifica in maniera univoca un certificato nell'ambito della CA che lo ha generato
Valid from/Valido dal	la data da cui il certificato può essere utilizzato;
Valid to/Fino A	specifica la data entro il quale il certificato può essere utilizzato. Assieme alla data di inizio determina il periodo di validità
Key usage/Utilizzo della chiave	descrive le aree d'uso della coppia di chiavi (firma della posta, autenticazione del client, …).
Digital signature/Firma Digitale	campo contenente la firma digitale generata dalla chiave privata della CA che ha rilasciato il certificato, con la quale si verifica l'identità del soggetto

Elementi del certificato: soggetto



Il soggetto del certificato è il possessore della chiave privata corrispondente alla chiave pubblica che è stata certificata:
Può essere:

- una persona fisica
- una persona giuridica
- un dispositivo, un sistema, un dominio
- una subCA

ma anche altro ad es. l'identificativo del mese nella marca temporale

ATTENZIONE: il soggetto/subject può non essere il richiedente/subscriber

Firma Digitale vs Firma Autografa

FIRMA AUTOGRAFA

a) **Direttamente** riconducibile al soggetto firmatario

b) Verifica **soggettiva** da parte di un terzo perito imparziale (attraverso il campione)

c) Facilmente **falsificabile** ma il falso è riconoscibile

d) Fa piena prova fino a querela di falso della **provenienza dichiarazioni** contenute nell'atto (ex art. 2702 cc)

e) In caso di disconoscimento **l'onere della prova** non spetta al firmatario

f) A un soggetto corrisponde **una sola firma**

FIRMA DIGITALE

a) Riconducibile al firmatario attraverso il possesso di un segreto

b) Verifica oggettiva da parte di un terzo imparziale (attraverso le chiavi)

c) Difficilmente **falsificabile**, ma il falso è irriconoscibile

d) Fa piena prova fino a querela di falso della **provenienza dichiarazioni** contenute nell'atto (ex art. 2702 cc)

e) In caso di disconoscimento **l'onere della prova** del non utilizzo del dispositivo spetta al firmatario (c.d. inversione dell'onere della prova)

f) Un soggetto può avere **più firme**

g) Una firma elettronica qualificata ha effetti giuridici **equivalenti** a quelli di una firma autografa.

Firma Digitale Remota

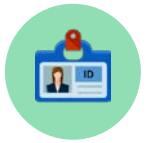
La **firma digitale remota** è un particolare tipo di firma digitale che è stata sviluppata per garantire un'elevata **User Experience** nel rispetto della normative sulla firma elettronica e digitale; custodita presso un provider remoto all'interno di un **HSM** (dispositivo crittografico hardware), su cui sono utilizzate le chiavi crittografiche necessarie per la generazione della firma digitale. Per accedere al dispositivo è necessario conoscere un PIN, che può essere generato da un dispositivo fisico (sistema **OTP**- One Time Password, cioè una password generata per una sola transizione) oppure dalla sim del proprio telefono cellulare.

connessa unicamente al **firmatario**

collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati (**integrità**)

rendere manifesta e di verificare la prove nienza un documento informatico (**paternità**)

basata su un su un sistema di chiavi crittograf iche, una pubblica e una privata



idonea a **identificare** il firmatario

basata su un **certificato qualificato** per firme elettroniche

creata da un dispositivo per la creazione di una firma elettronica qualificata e mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo

Certificazione

La **Firma Elettronica Qualificata**, categoria in cui rientra la Firma Digitale, è una firma basata, tra l'altro, su dei **certificati** qualificati: si tratta di uno strumento elettronico rilasciato da un Qualified Trust Service Provider (**QTSP**, introdotto dal Regolamento Europeo n. 910/2014, comunemente detto **eIDAS**). Questo strumento serve a garantire rispettivamente

Certificato di **sottoscrizione**: è necessario per la **Firma Digitale**, permette di apporre la firma ed è graficamente riconoscibile dalla coccarda. È identificato dalla dicitura **PRA**

Certificato di **autenticazione (e CNS)**: permette autenticazione a siti web e firma della propria posta elettronica (S/MIME). È identificato dalla dicitura **AUT**

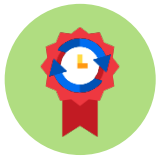
Certificato di sottoscrizione con **ruolo**: è un certificato di sottoscrizione arricchito di informazioni di appartenenza a un particolare ordine professionale, categoria o con specifici poteri di rappresentanza

Gestione dei Certificati

Il QTSP svolge il ruolo di **certificatore**, e quindi:

Genera i certificati per i **titolari registrati** (tre dati fondamentali: CF, …)

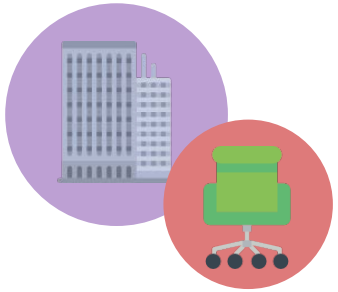
Pubblica i certificati (solo su richiesta)



Permette **prima della scadenza** il rinnovo (infocert certificato di firma vale 3 anni, se non si rinnova bisogna rifare il certificato)

Revoca i certificati non più validi (propria iniziativa, richiesta titolare, richiesta terza parte)

Soggetti interessati alla procedura - I



InfoCert è il Trust Service provider che emette, pubblica e revoca i certificati: opera in conformità di eIDAS e CAD. è iscritta dal 19 luglio 2007 nell'Albo dei Certificatori tenuto da AgID, e nel linguaggio corrente viene anche definito terza parte fidata: infatti quando si appone la firma si fa affidamento sul fatto che il **TSP** o i suoi delegati abbiano costruito un processo sicuro e l'abbiano posto in essere in modo corretto e legale.

Il **TSP** garantisce che la **chiave pubblica** e il codice Utente (IUT) siano univoci nel proprio dominio, pubblica su richiesta il certificato e garantisce la sussistenza di poteri o titoli in capo al Titolare.

Da ultimo il TSP redige e aggiorna la lista revoca o sospensione (**CRL**) dei certifcati.

Il **RAO** e l **IR** sono l'interfaccia di InfoCert verso il **titolare**: devono garantire di eseguire le operazione di identificazione e emissione del certificato secondo le istruzioni e la formazione ricevute dal TSP.

Verificano aspetti formali (condizioni di emissione del certificato e documenti di identità), garantisce riconoscimento del soggetto, per attivare procedura di emissione. Inoltre informano il Titolare richiedente sugli obblighi di protezione della segretezza della chiave privata.

A loro volta i RAO devono custodire con la massima cura il dispositivo di firma contenete certificati RAO, il PIN e la busta di revoca.

Soggetti interessati alla procedura - II

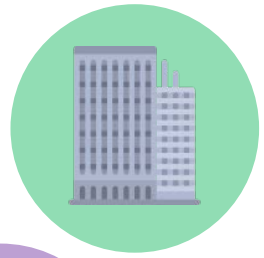
Il **Titolare** deve essere una **persona fisica**, di cui devono essere raccolti nome e cognome, età (è necessario che sia maggiorenne) e sia provvisto di con CF o identificativo equivalente (cioè il codice generato all'interno della struttura burocratica del paese di provenienza). Al **titolare** è attribuita la firma e Il suo nome risulta all'interno del certificato quello il cui nome è all'interno del certificato e a cui è attribuita la firma. Sul titolare incombe l'obbligo di:

a) **custodire** con la massima cura la chiave privata (ovvero il dispositivo di firma) e il PIN
b) **conservare** il codice di emergenza (ERC)
c) fare un **uso esclusivo** del dispositivo di firma

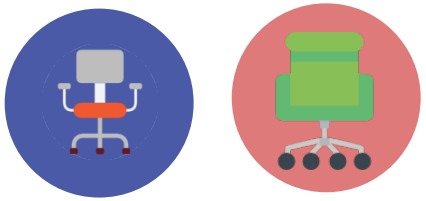
Il **terzo interessato** è l'ente che può attribuire un titolo o un ruolo al Titolare: al momento del riconoscimento, infatti, può essere rilasciato un certificato con **ruolo** che fa, appunto, riferimento ai **poteri** o **compiti** spettanti al Titolare all'interno dell'organizzazione.

RAO e IR

InfoCert, attraverso apposite convenzione, nomina e forma gli Uffici di Registrazione (**RAO**)

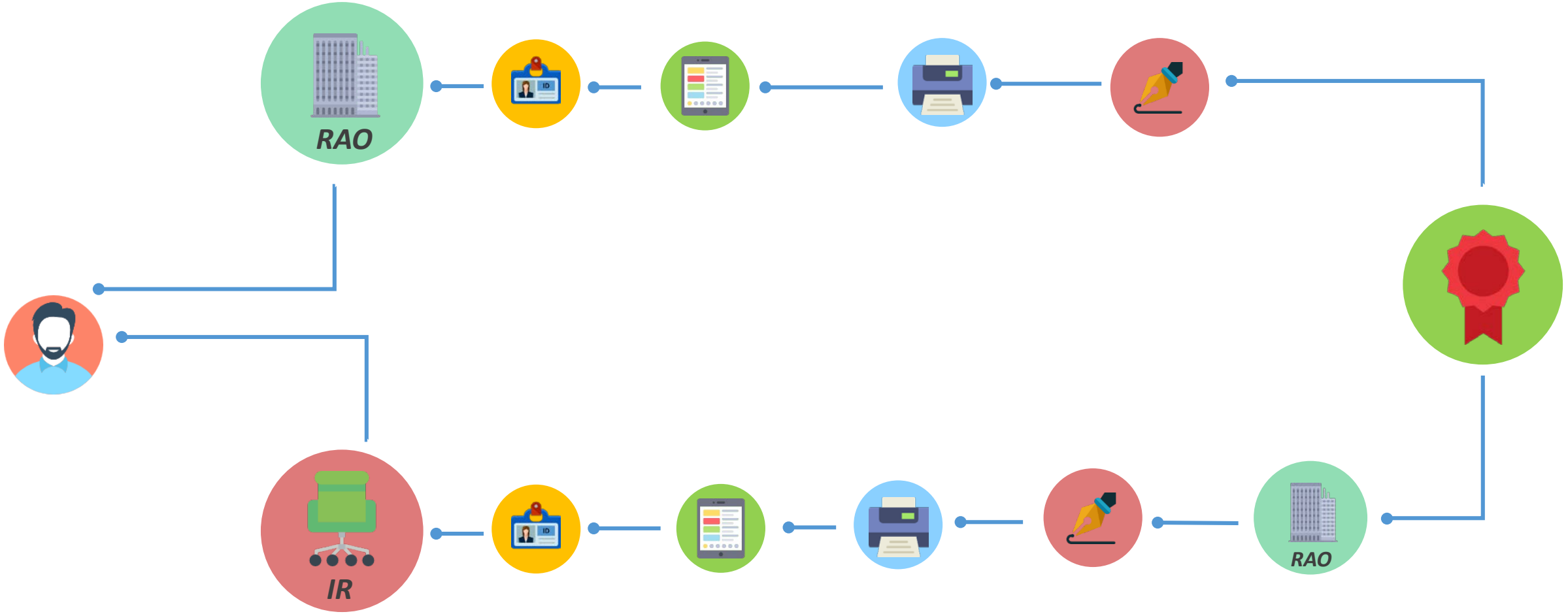


I RAO, attraverso apposite convenzione, nominano e formano gli Incaricati alla Registrazione (**IR**)



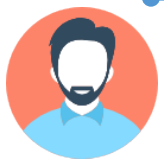
Gli utenti possono essere **identificati** tanto dai RAO quanto dagli IR, ma solo i primi possono rilasciare un certificato, generati da InfoCert (terza parte fidata)

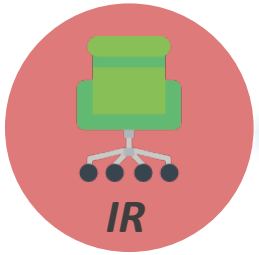
Emissione certificato



Avvio Procedura

in entrambi i casi è possibile **prenotare** sul sito un appuntamento per l'identificazione e rilascio





AVVIO DELLA PROCEDURA

Ready o post card

L'Utente può presentarsi per il rilascio del certificato (di autenticazione o sottoscrizione) al RAO e all'IR, nel primo caso si ha un procedimento readycard, in cui identificazione e rilascio di dispositivo e certificato avvengono nello stesso momento, nel secondo caso viene effettuata solo l'identificazione mentre certificato e dispositivo sono rilasciati in un momento successivo. Il procedimento postcard risulta utile quando vi sia:

a) zone geograficamente ampie

b) indisponibilità momentanea di strumenti informatici

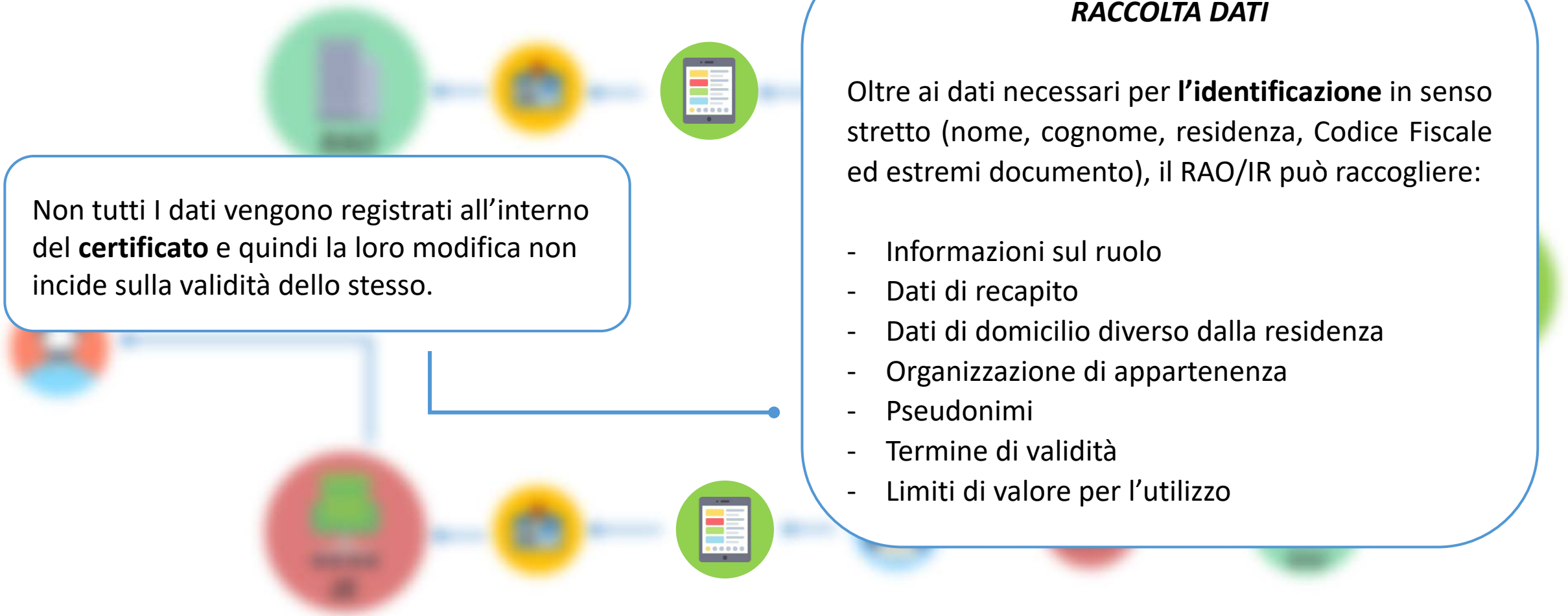
c) necessità di razionalizzazione del lavoro

Identificazione

IDENTIFICAZIONE del richiedente

- Richiesta al primo rilascio
- Fase cruciale della procedura
- Presenza fisica del richiedente (**no delega**)
- Controllo documento d'identità in corso di validità ex art. 35 L. **n.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 il passaporto o la carta di identità italiana (se cittadini comunitari). Il TIN (*Tax Identification Number*) è il numero di identificazione nazionale assegnato dei paesi dell'UE ai propri cittadini, con finalità di identificazione nel servizio fiscale nazionale.
- Attestazione del ruolo (eventuale)

Raccolta dati



Non tutti I dati vengono registrati all'interno del **certificato** e quindi la loro modifica non incide sulla validità dello stesso.

RACCOLTA DATI

Oltre ai dati necessari per **l'identificazione** in senso stretto (nome, cognome, residenza, Codice Fiscale ed estremi documento), il RAO/IR può raccogliere:

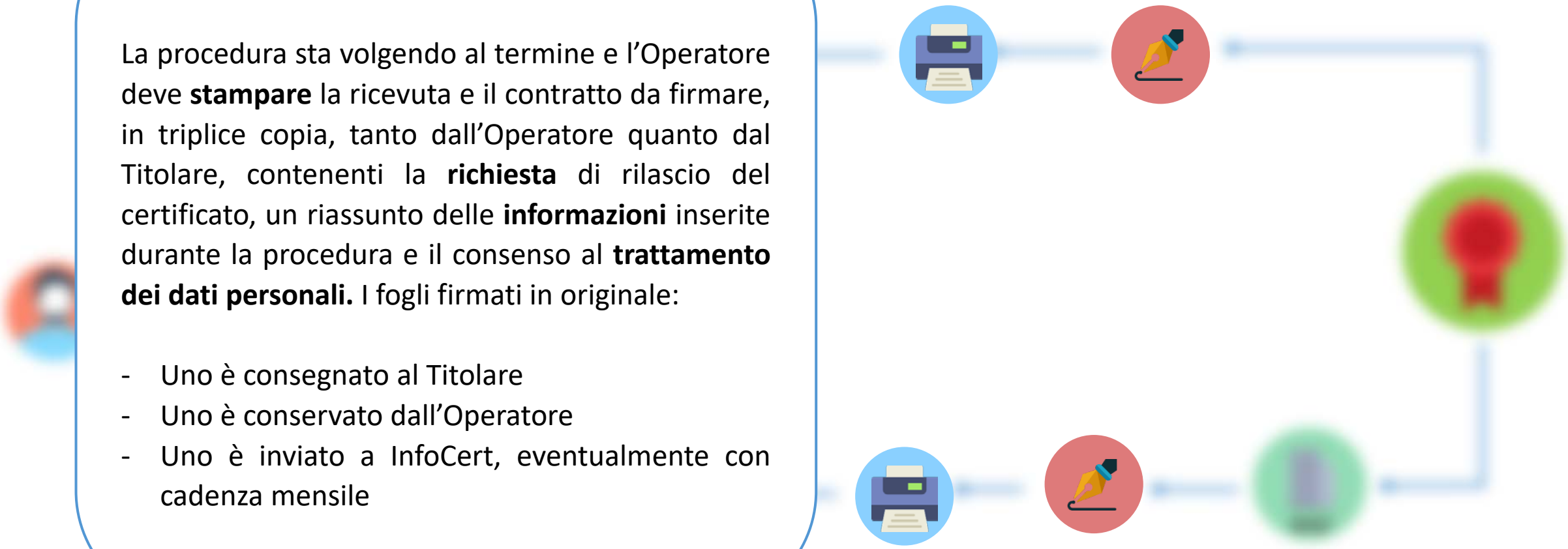
- Informazioni sul ruolo
- Dati di recapito
- Dati di domicilio diverso dalla residenza
- Organizzazione di appartenenza
- Pseudonimi
- Termine di validità
- Limiti di valore per l'utilizzo

Stampa e sottoscrizione

FIRMA

La procedura sta volgendo al termine e l'Operatore deve **stampare** la ricevuta e il contratto da firmare, in triplice copia, tanto dall'Operatore quanto dal Titolare, contenenti la **richiesta** di rilascio del certificato, un riassunto delle **informazioni** inserite durante la procedura e il consenso al **trattamento dei dati personali.** I fogli firmati in originale:

- Uno è consegnato al Titolare
- Uno è conservato dall'Operatore
- Uno è inviato a InfoCert, eventualmente con cadenza mensile



PostCard vs readyCard

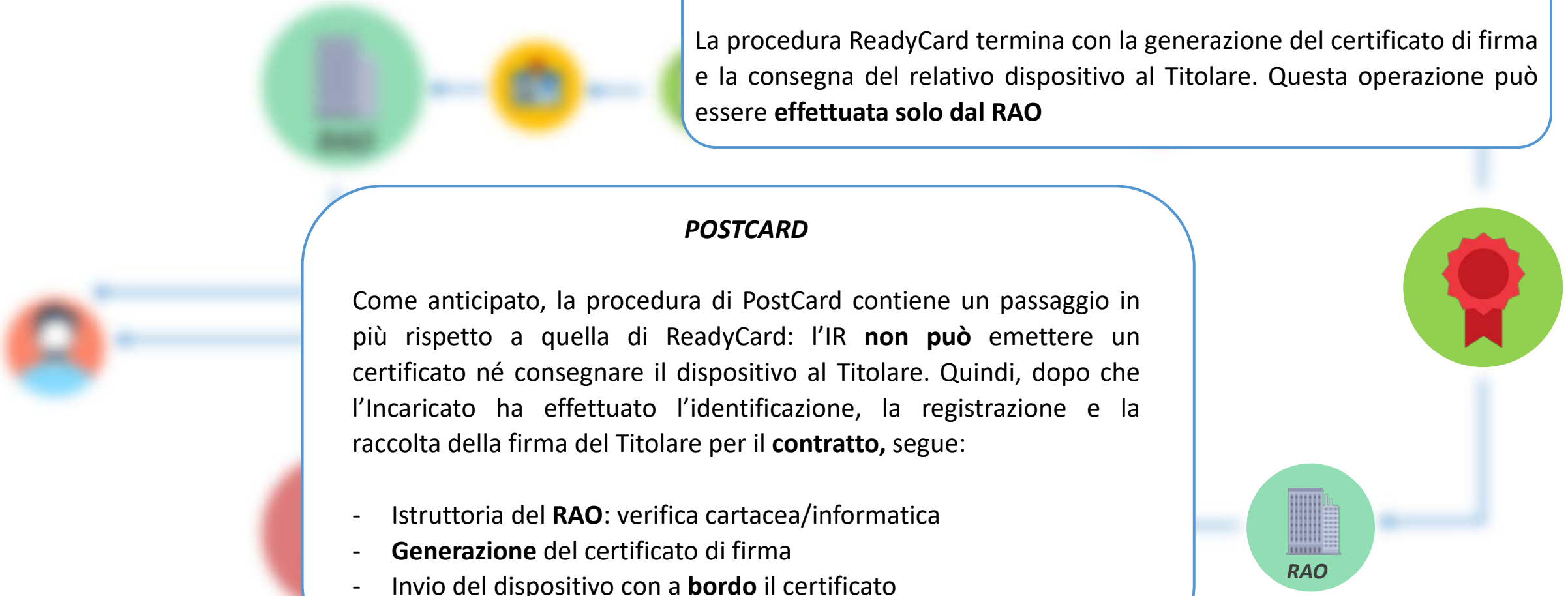
READYCARD

La procedura ReadyCard termina con la generazione del certificato di firma e la consegna del relativo dispositivo al Titolare. Questa operazione può essere **effettuata solo dal RAO**

POSTCARD

Come anticipato, la procedura di PostCard contiene un passaggio in più rispetto a quella di ReadyCard: l'IR **non può** emettere un certificato né consegnare il dispositivo al Titolare. Quindi, dopo che l'Incaricato ha effettuato l'identificazione, la registrazione e la raccolta della firma del Titolare per il **contratto,** segue:

- Istruttoria del **RAO**: verifica cartacea/informatica
- **Generazione** del certificato di firma
- Invio del dispositivo con a **bordo** il certificato
- In ogni caso, raccolta della firma del Titolare per la **ricevuta**



PostCard vs readyCard

AUTENTICAZIONE

In caso di **sospensione** o **revoca** richiesta dal titolare sarà necessaria l'**autenticazione**: per questo motive I certificate di sottoscrizione (PRA) vengono spesso emessi insieme a un certificato di autenticazione (AUT).

CERTIFICATO

Il **certificato** normalmente viene emesso con validità triennale ed è valido fino a:

- **Sospensione**: il certificato può essere sospeso per un determinato periodo, su richiesta di parte o d'ufficio. Al termine della sospensione riacquista validità e **non rimane traccia** dell'operazione di sospensione;
- **Revoca:** il certificato può essere revocato solo presso **l'ufficio** del RAO, che esegue la procedura e emette la relativa ricevuta. La revoca avviene su richiesta di parte o d'ufficio;
- **Scadenza:** al termine previsto il certificato perde validità. È possibile rinnovare il certificato tra i **90 giorni e il giorno prima** la data di scadenza: decorso tale termine bisogna richiedere un nuovo certificato **.**

Sospensione, revoca, rinnovo

SOSPENSIONE

-su richiesta di parte, di terzi o d'ufficio
-valida dalla pubblicazione nella lista **CRL** (lista certificate revocati o sospesi), che si **aggiorna** ogni ora
-temporanea
-al termine del periodo di sospensione il certificato è considerate come sempre valido
-un certificato sospeso può essere **revocato** o **ripristinato** prima del termine
- **motivi**: dubbi su validità del certificato o autenticità della richiesta di revoca, nonché necessità di interromperne la validità.

REVOCA

-Su richiesta di parte, di terzi o d'ufficio
-valida dalla pubblicazione nella lista **CRL** (lista certificate revocati o sospesi), che si **aggiorna** ogni ora
-definitiva
-un certificato revocato **non può** essere sospeso
-**motivi**: chiave privata compromessa, gusto dispositivo, cambio dati titolari presenti nel certificato, disdetta, non rispetto del Manuale Operativo

RINNOVO

-possibile da 90 a 1 giorno prima della scadenza
-online nel negozio InfoCert o presso un RAO
-se non viene eseguito il rinnovo il certificato scade e deve esserne acquistato uno nuovo ripetendo la procedura

Inizializzazione del dispositivo di firma

Una volta **emesso** il certificato, il dispositivo può essere inizializzato con il software **DIKE 6**.
Al titolare vengono consegnati:

N. 1 **dispositivo di firma**

N. 1 **cartellina** contenente - sotto la scratch area – i seguenti codici:

a) Codice di Emergenza: 10 cifre da utilizzare in caso di richiesta di **sospensione** del certificato

b) Codice **PIN**: necessario per attivare il dispositivo e liberare la chiave private. Questo codice deve essere modificato al primo utilizzo del dispositivo

c) Codice **PUK**: necessario in caso di blocco del PIN

N. 3 **documenti**: Ricevuta dell'operazione, Contratto ed estratto del Manuale Operativo

Inizializzazione certificato di firma remota

Una volta **registrati i dati** da parte del RAO, il certificato di firma remota di può essere attivato sul portale My Sign. Al titolare vengono consegnati:

N. 1 **e-mail** con le informazioni e le istruzioni per attivare il certificato

N. 1 **cartellina** contenente - sotto la scratch area – i seguenti codici:

a) Codice di Emergenza: 10 cifre da utilizzare in caso di richiesta di **sospensione** del certificato

b) Codice **PIN**: necessario per attivare il dispositivo e liberare la chiave private. Questo codice deve essere modificato al primo utilizzo del dispositivo

c) Codice **PUK**: non utilizzabile per la firma remota

N. 3 **documenti**: Ricevuta dell'operazione, Contratto ed estratto del Manuale Operativo

Manuale Operativo

Il **Manuale Operativo**, consultabile online, contiene la descrizione delle procedure applicate dall'Ente Certificatore InfoCert per rilasciare e gestire i certificati.
E' **pubblicato su Internet** e risponde ad un preciso obbligo di legge.
In effetti, esistono tanti Manuali Operativi per quante sono le tipologie di certificati gestiti.

Manuale RAO

Il **Manuale RAO**, consultabile online, contiene le indicazioni per l'utilizzo dell'interfaccia di registrazione e emissione dei certificati (**NCAR**).
Sul sito di Assistenza Clienti sono disponibili le guide per l'uso del software di firma (**DIKE 6**)

Attivare dispositivo di firma (**cambiando** anche il PIN al primo utilizzo)

Apporre/verificare una o più firme su **qualsiasi tipo di file**

Apporre **marca temporale** (data certa, necessaria per poter provare che la firma è stata apposta nel periodo di validità del certificato)

Il documento firmato ottiene estensione **P7M** o **PDF**

Grazie.

www.infocert.it