Università degli Studi di Napoli Federico II

Servizi per l'eGovernment

C.S.I. – Centro di Ateneo per i Servizi Informativi

Area Tecnica eGovernment

La diffusione della firma digitale in Ateneo

Napoli, 4 novembre 2013

Il Codice dell'amministrazione digitale e la firma digitale

- Il documento informatico sottoscritto con **firma digitale**
  - ✓ soddisfa il requisito legale della forma scritta,
  - ✓ ha efficacia giuridico-probatoria.

- La firma digitale garantisce autenticazione, non ripudio (fino a querela di falso da parte del sottoscrittore) e l'integrità del documento informatico sottoscritto.

- L'uso della firma digitale integra e sostituisce ad ogni fine di legge l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti.

La firma digitale - Generalità

- La firma digitale è basata su un procedimento di "crittografia asimmetrica" che fa uso di una coppia di chiavi: una privata (utilizzata per firmare) ed una pubblica (utilizzata per le operazioni di verifica della firma).
- La corrispondenza tra le chiavi di firma ed il sottoscrittore è garantita da una terza parte fidata, il certificatore qualificato.
- Il certificatore (qualificato) genera e consegna a ciascun titolare un dispositivo sicuro di firma contenente: la coppia di chiavi assieme ad un certificato qualificato di firma che consente l'associazione della persona con la sua chiave pubblica.
- Il certificatore (qualificato) gestisce l'identificazione e la registrazione certa del richiedente, nonchè la sospensione temporanea della validità o la revoca definitiva del certificato qualificato.

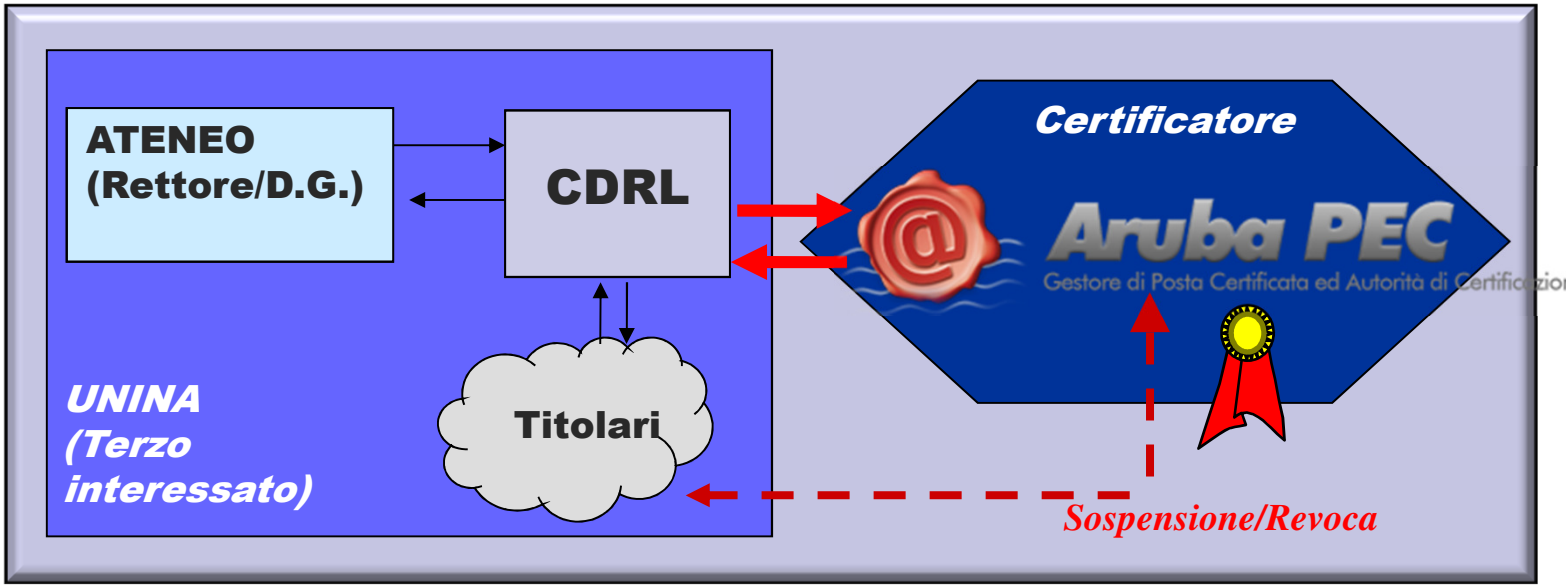
Il servizio firma digitale dell'Ateneo (1/2)

- L'Ateneo, in qualità di "terzo interessato", si avvale dei servizi offerti dal **certificatore accreditato** **ARUBAPEC SpA**.
- Il servizio si basa sulla organizzazione di una "Registration Authority" interna, denominata "**Centro di Registrazione Locale (CDRL)** ", costituita da amministrativi dell'Ateneo all'uopo nominati dal Rettore su indicazione dei Direttori di Dipartimento e quindi delegati dal Certificatore.
- I dispositivi sicuri di firma, contenenti la chiave crittografica di sottoscrizione ed il certificato del titolare, sono **SIM** all'interno di lettori di tipo "**token USB**".
- I certificati qualificati sono assegnati ai responsabili di struttura, ai docenti e ricercatori, ai dirigenti e capi ufficio o ad altri soggetti, secondo le indicazioni fornite dal Rettore e dal Direttore Generale.
- La firma digitale, integrata nell'architettura funzionale e di servizio per l'eGovernment dell'Ateneo deve essere utilizzata per la sottoscrizione di documenti amministrativi informatici.

Il servizio firma digitale dell'Ateneo (2/2)

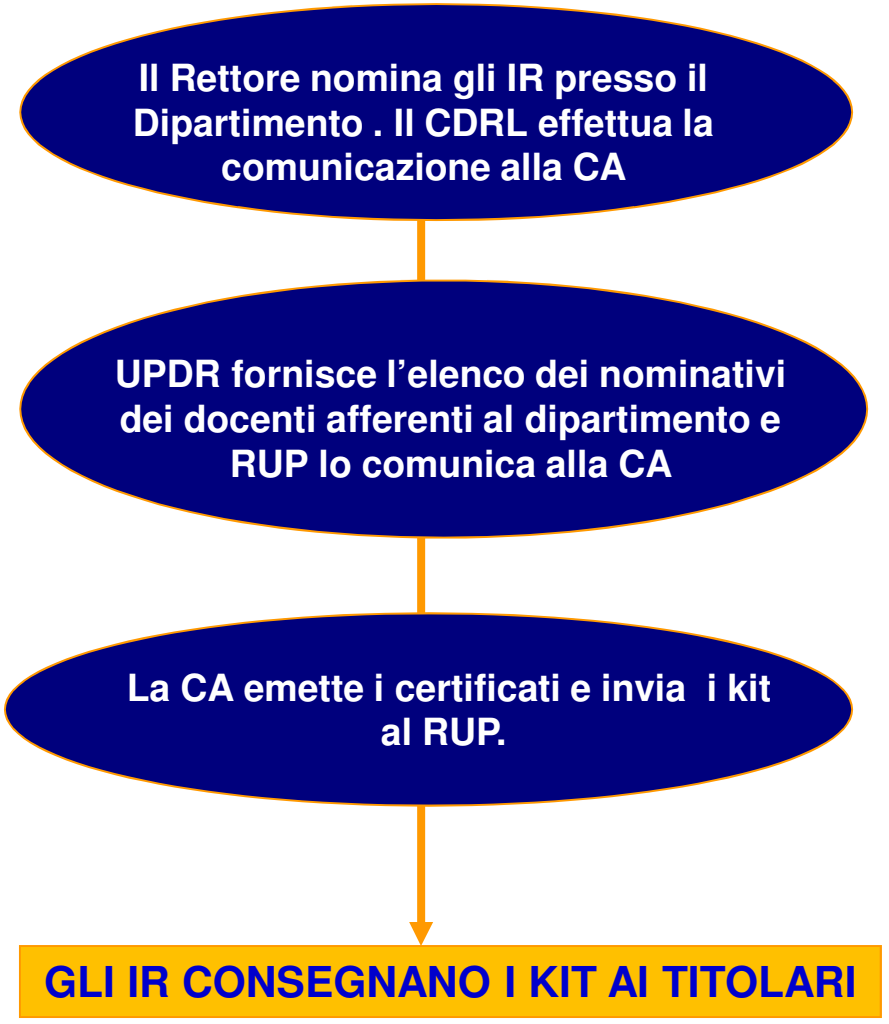
- **Il Regolamento di Ateneo (DR 4064 del 31.10.2006) in materia di Firma Digitale, definisce:**
  - ✓ **Regole per l'assegnazione, la sospensione e la revoca dei certificati da parte dell'Ateneo,**
  - ✓ **Compiti e responsabilità dell'Ateneo (nella figura della propria «Registration Authority» interna, nel seguito, «CDRL») nei confronti del Certificatore, e dei Titolari di certificato qualificato,**
  - ✓ **Diritti dell'Ateneo, in qualità di "terzo interessato" e adempimenti dei Titolari,**
  - ✓ **Regole per la sottoscrizione e la tenuta dei documenti amministrativi digitali**

Il Centro Di Registrazione Locale (CDRL) (1/2)



Il Centro Di Registrazione Locale (CDRL) (2/2)

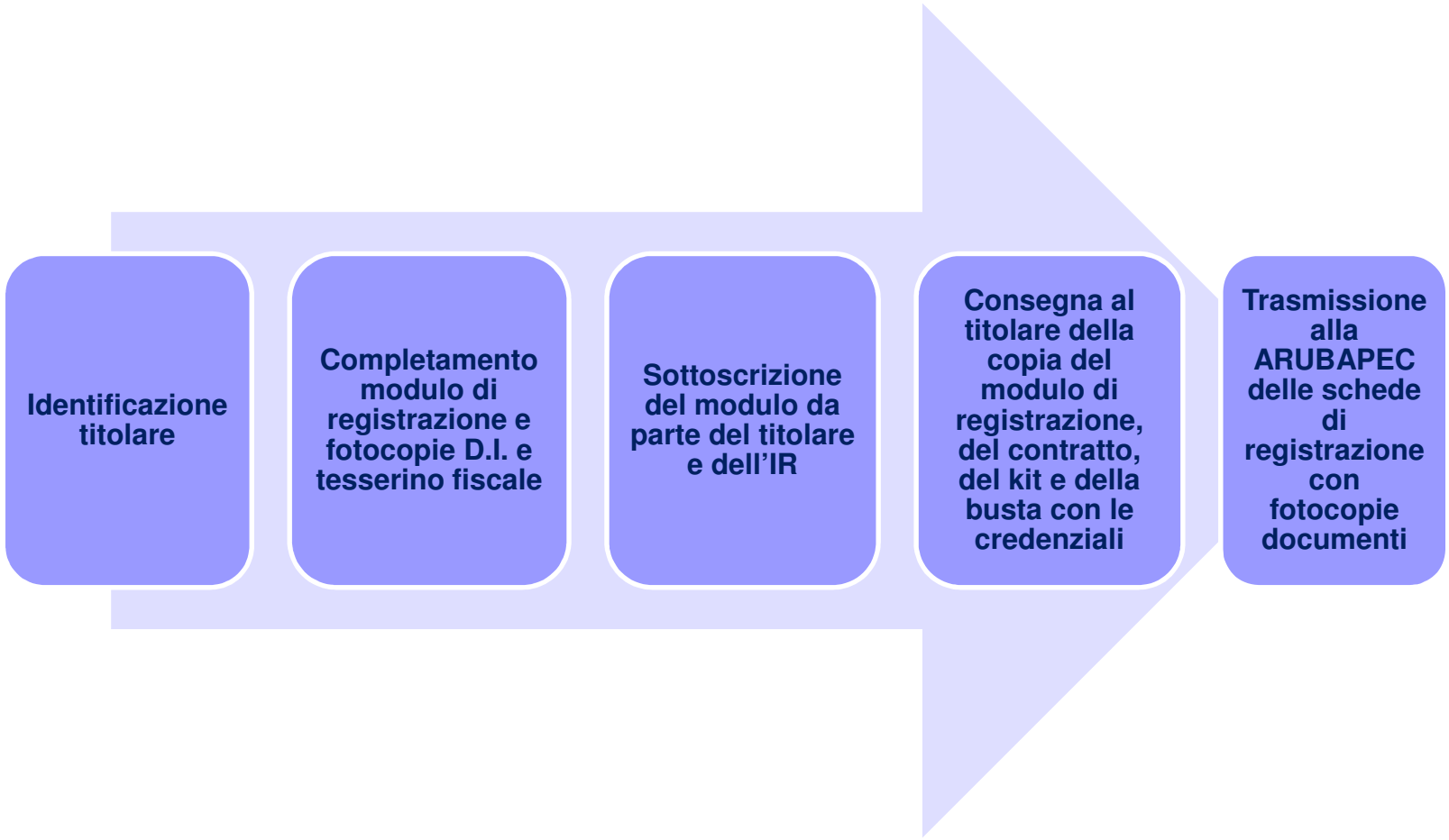
L’emissione dei certificati in modalità «bulk»



La fase di registrazione e di consegna dei kit di firma (1/2)

- **Gli IR presso ciascun dipartimento/scuola hanno a disposizione l'elenco dei titolari di firma;**
- **Per ciascun titolare, all'atto della consegna, associano a ciascuna scheda contenente la SIM personalizzata la busta contenente: la scheda di registrazione, una copia del contratto e la busta oscurata con PIN/PUK;**
- **La scheda di registrazione contenuta nella busta viene completata con gli estremi del documento di riconoscimento del titolare e sottoscritta dal titolare (3 firme) e dall'IR;**
- **Viene effettuata una fotocopia del documento di identità, del tesserino con il CF e della scheda di registrazione;**
- **La copia della scheda di registrazione viene consegnata al titolare insieme al contratto, al box con il token e alla busta oscurata;**
- **Le schede di registrazione sono inviate a mezzo corriere alla Arubapec.**

La fase di registrazione e di consegna dei kit di firma (2/2)



Le condizioni generali del contratto

- Definizione dei quattro ruoli: CA, Terzo interessato (Università), Committente (CSI), Utente;
- Contratto non a titolo oneroso tra CA e Utente;
- Il riferimento è all'accordo tra CA e CSI (RDO 97213) per la fornitura di 3200 kit di firme e relativi servizi;
- La durata dei certificati è pari a 6 anni, rinnovabili di ulteriori 6 anni;
- Un certificato può essere revocato:
  - Su indicazione dell'Ateneo,
  - Su richiesta del titolare,
  - Per volontà della CA;
- In ogni caso, viene informata anche la struttura di partenza;
- Foro competente: Napoli.

La sospensione/revoca dei certificati

CA

- Comunica l'avvenuta revoca all'l'interessato e al CDRL. Il CDRL informa la struttura di afferenza.

Titolare

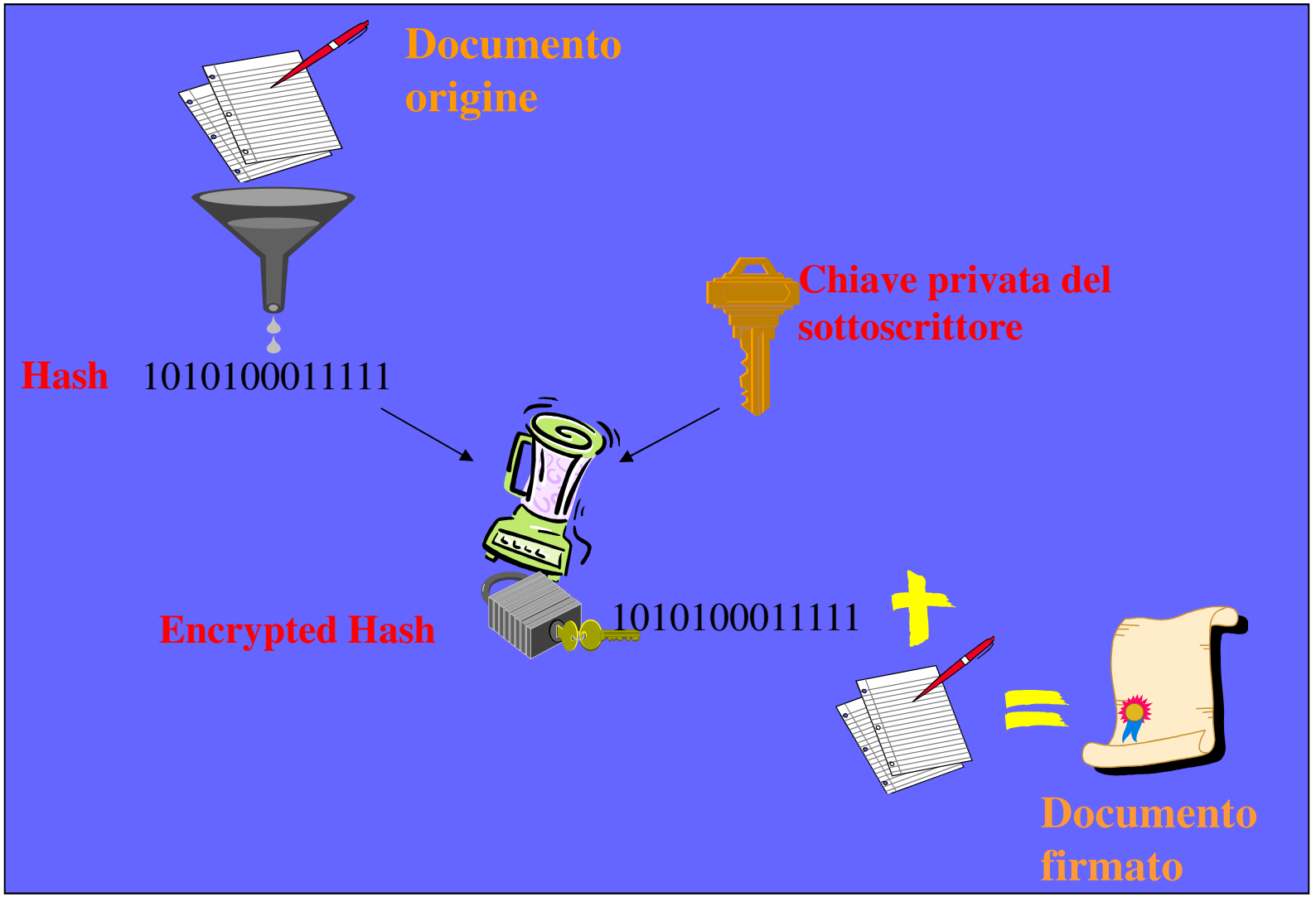
- Comunica la richiesta di revoca/sospensione alla CA e informa il CDRL e la propria struttura di afferenza. In ogni caso, la richiesta viene notificata al CDRL anche dalla CA. Il CDRL si attiva per la ri-emissione del certificato.

CDRL

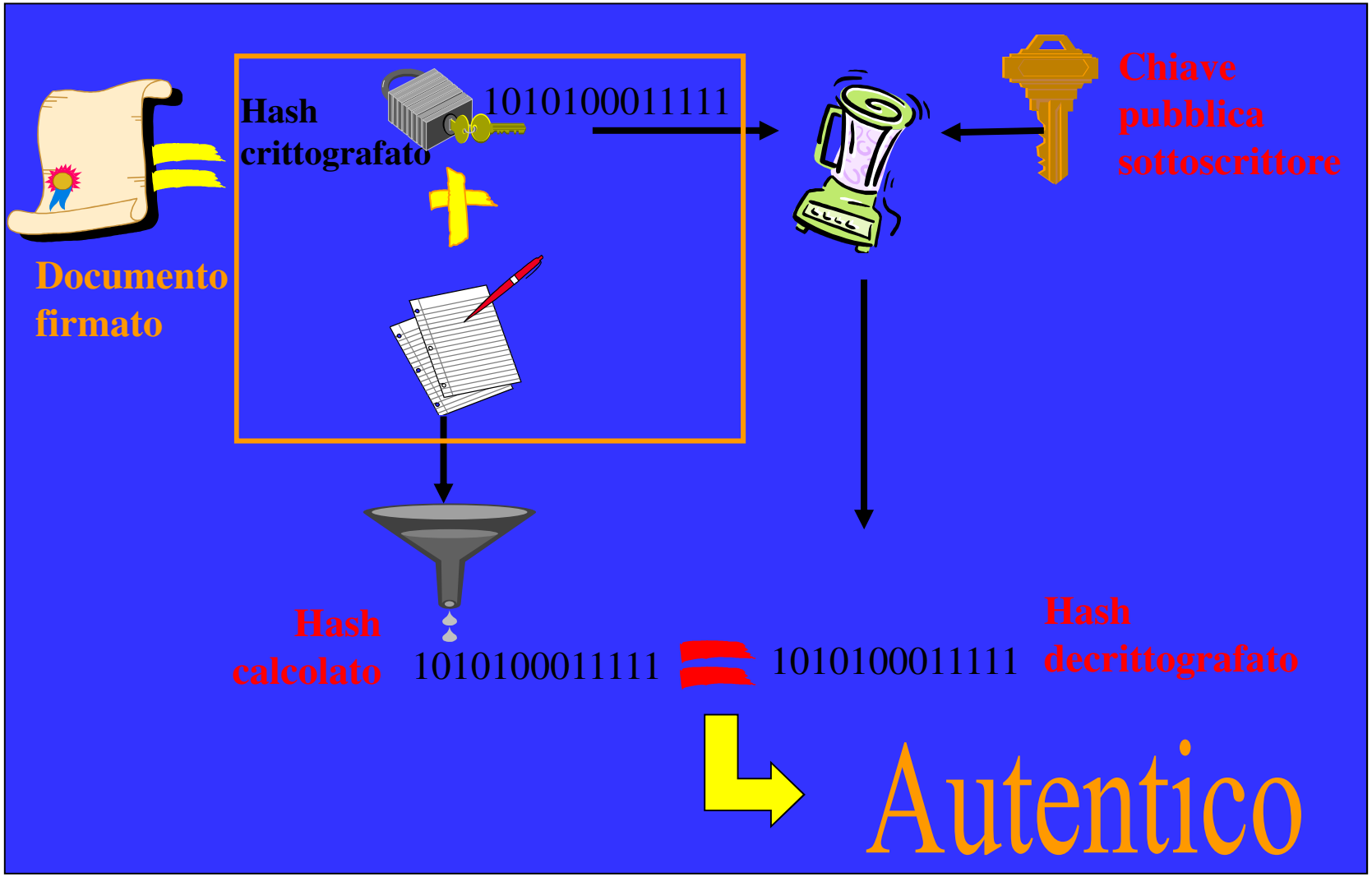
- Procede su indicazione dell'Ateneo e ne dà comunicazione anche alla struttura di afferenza del titolare.

Il processo di apposizione della firma digitale (1/2)

Il processo di apposizione della firma digitale (2/2)



Il processo di verifica della firma digitale (2/2)

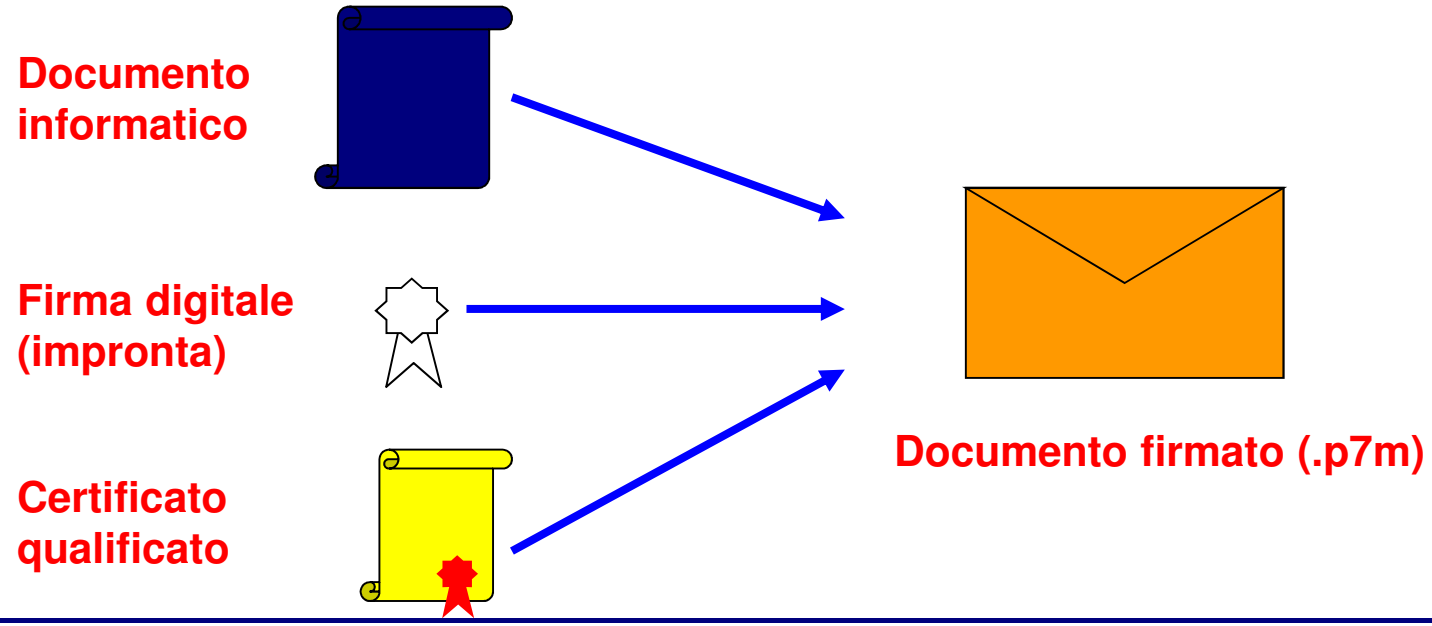


Il certificato qualificato

- Il certificato di firma è un documento elettronico che, oltre a contenere i dati essenziali del titolare, ne contiene la chiave pubblica:

Il formato di firma

- Il documento da firmare è imbustato nel formato originale, senza aggiunte in testa o in coda al formato stesso. Il file firmato, ossia la busta, contiene al suo interno:
  - **il documento informatico nel formato originale,**
  - **la firma digitale ad esso associata (l'impronta),**
  - **il certificato qualificato del sottoscrittore.**



Come apporre e verificare la firma digitale

- Il titolare deve apporre in chiaro, nel documento, il proprio ruolo, il nome, il cognome e la data di sottoscrizione.
- Il titolare deve trasformare il documento informatico in formato pdf, eventualmente adoperando strumenti di tipo "open source" oppure «freeware», scaricabili anche dal sito www.praxis.unina.it.
- Per firmare il documento, è sufficiente eseguire l'applicazione di apposizione della firma digitale disponibile nella toolbar della ARUBAKEY.
- Il file ".p7m" ottenuto può quindi essere conservato su supporto magnetico, oppure trasmesso mediante strumenti telematici (Posta Elettronica o Posta Elettronica Certificata).
- La verifica di autenticità e di integrità del file firmato può essere eseguita con un qualunque strumento di verifica (ad esempio, i prodotti ArubaSign oppure, DigitaSign reader) di libera e gratuita disponibilità.

Il certificato per l'autenticazione ai servizi in rete

- A bordo delle SIM è presente anche un certificato «CNS like» per l'autenticazione dei titolari ai servizi informatici dell'Ateneo.
- Il dispositivo è compatibile con quelli previsti dall'art. 64 comma 2 del Codice per l'Amministrazione Digitale (CAD) per l'accesso ai servizi in rete della PA e contiene, tra gli altri dati, il codice fiscale del titolare della carta e la denominazione dell'Università quale terzo interessato.
- Ai sensi dell'art. 65 del CAD, le istanze e le dichiarazioni presentate dagli interessati per via telematica siano valide ed equivalenti alle istanze e dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento se i richiedenti si autenticano al sistema informativo dell'Ateneo utilizzando tale certificato digitale di autenticazione.