CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Il codice della amministrazione digitale: aspetti tecnologici.

Giovanni Manca
Ufficio Standard e tecnologie d'identificazione

AGENDA

- **Decreto legislativo, 4 aprile 2006, n. 159.**
- **Principi fondamentali della firma digitale.**
- **Dematerializzazione**
- **La PEC – Posta elettronica certificata: modalità tecniche di trasmissione e di ricezione.**
- **L'architettura del Sistema Pubblico di Connettività.**

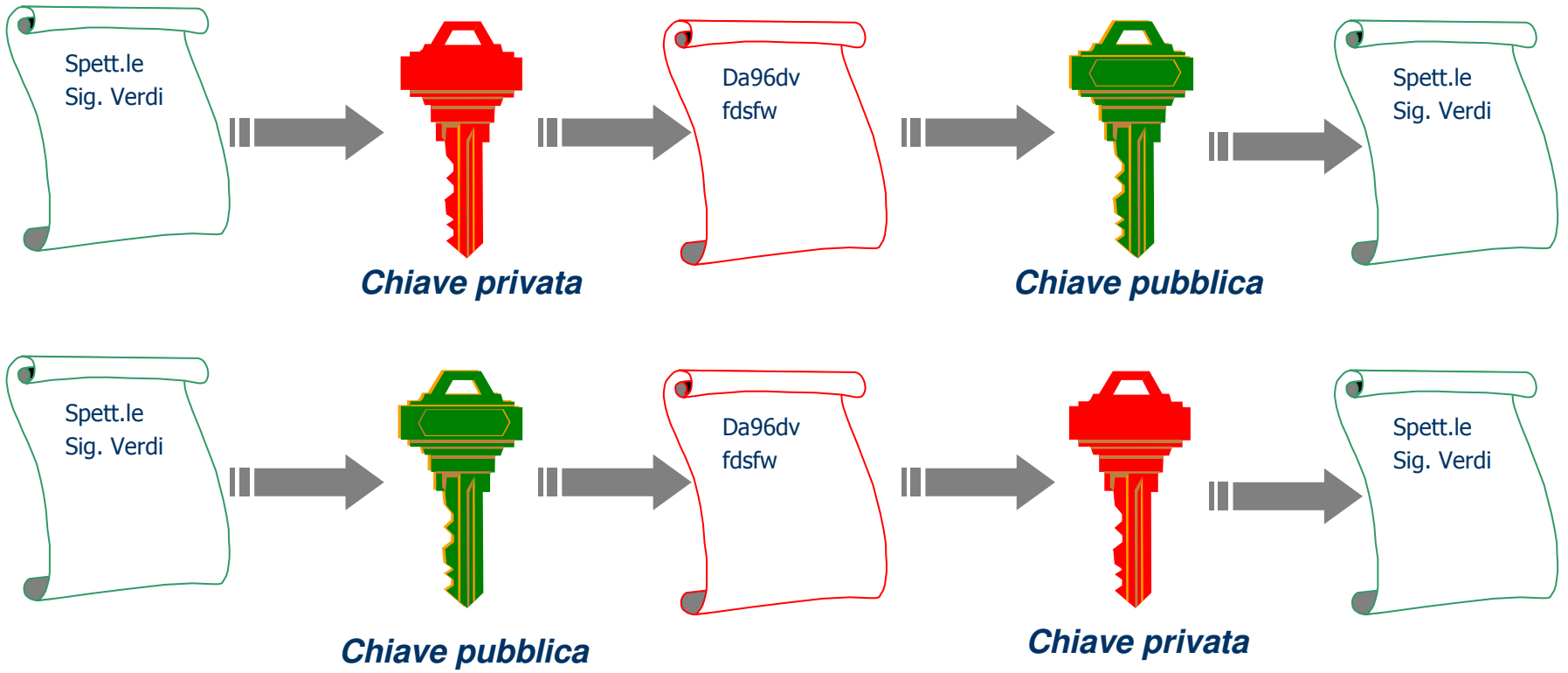
Principi fondamentali della firma digitale

Le chiavi e la crittografia asimmetrica

Chiave pubblica

Chiave privata

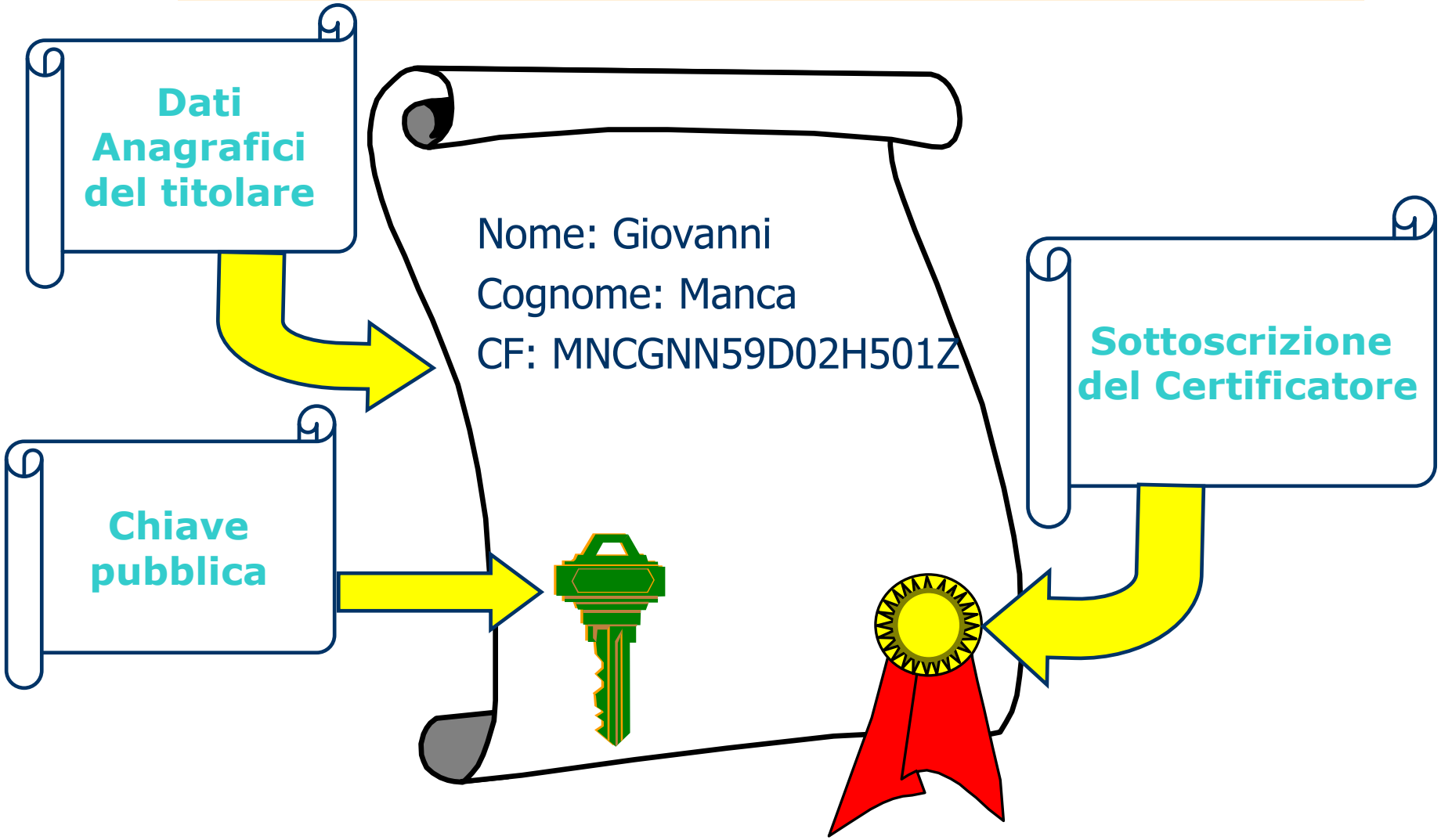
Le chiavi e la crittografia asimmetrica



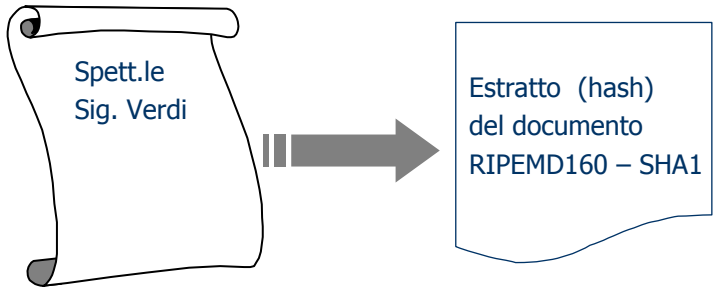
Le chiavi sono complementari

Generazione della firma digitale

Il Certificato



La generazione della Firma



La funzione di Hash

Produce sempre 160 bit (40 caratteri)

Non è reversibile

Non è possibile produrre collisioni utili

La funzione di Hash

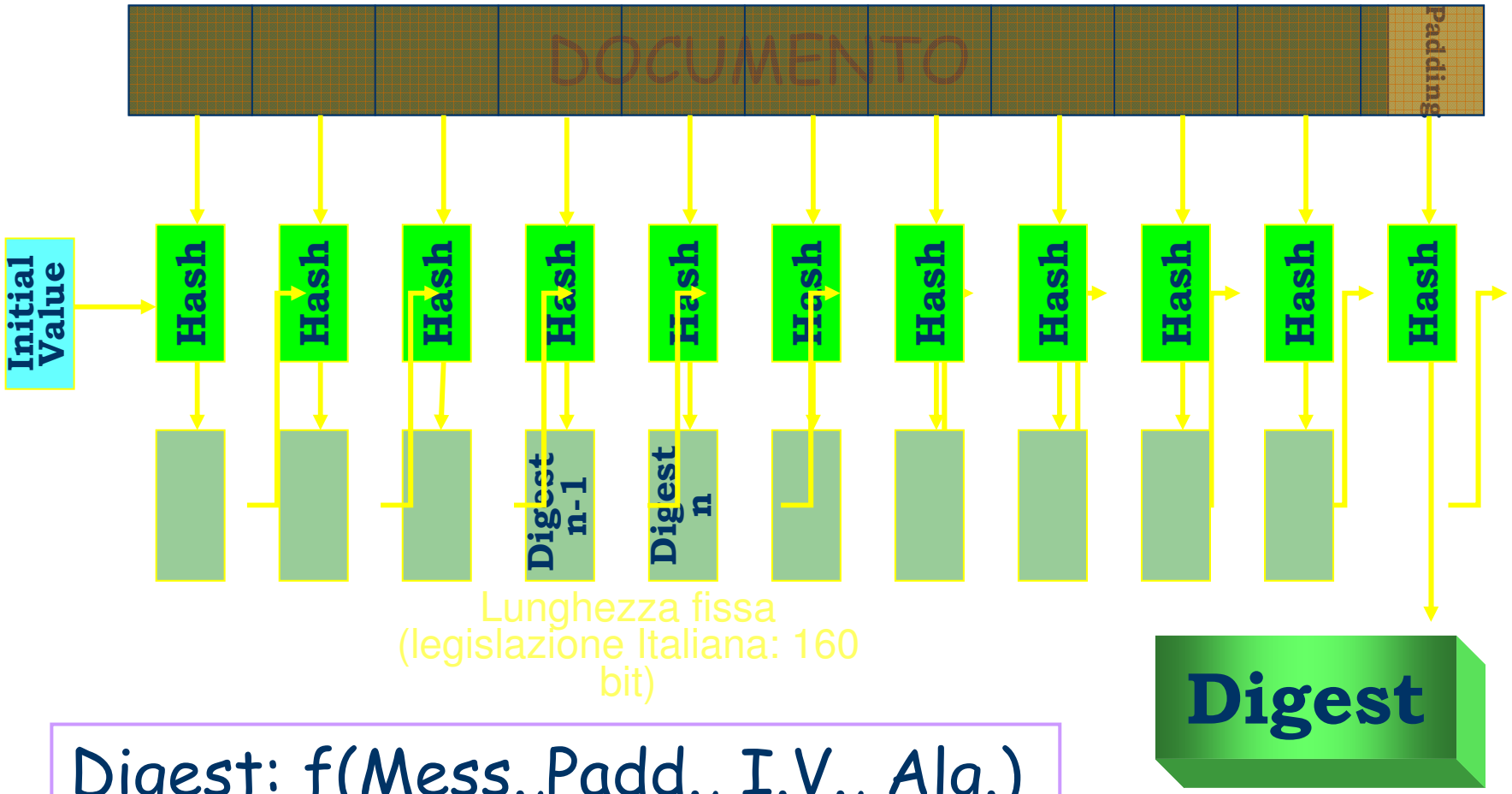
Recentemente alcuni matematici hanno individuato una "via agevolata" per produrre collisioni.

Questo consente di ridurre i tentativi da 2^80 a

2^69 cioè "solo" 590 miliardi di miliardi di tentativi circa.

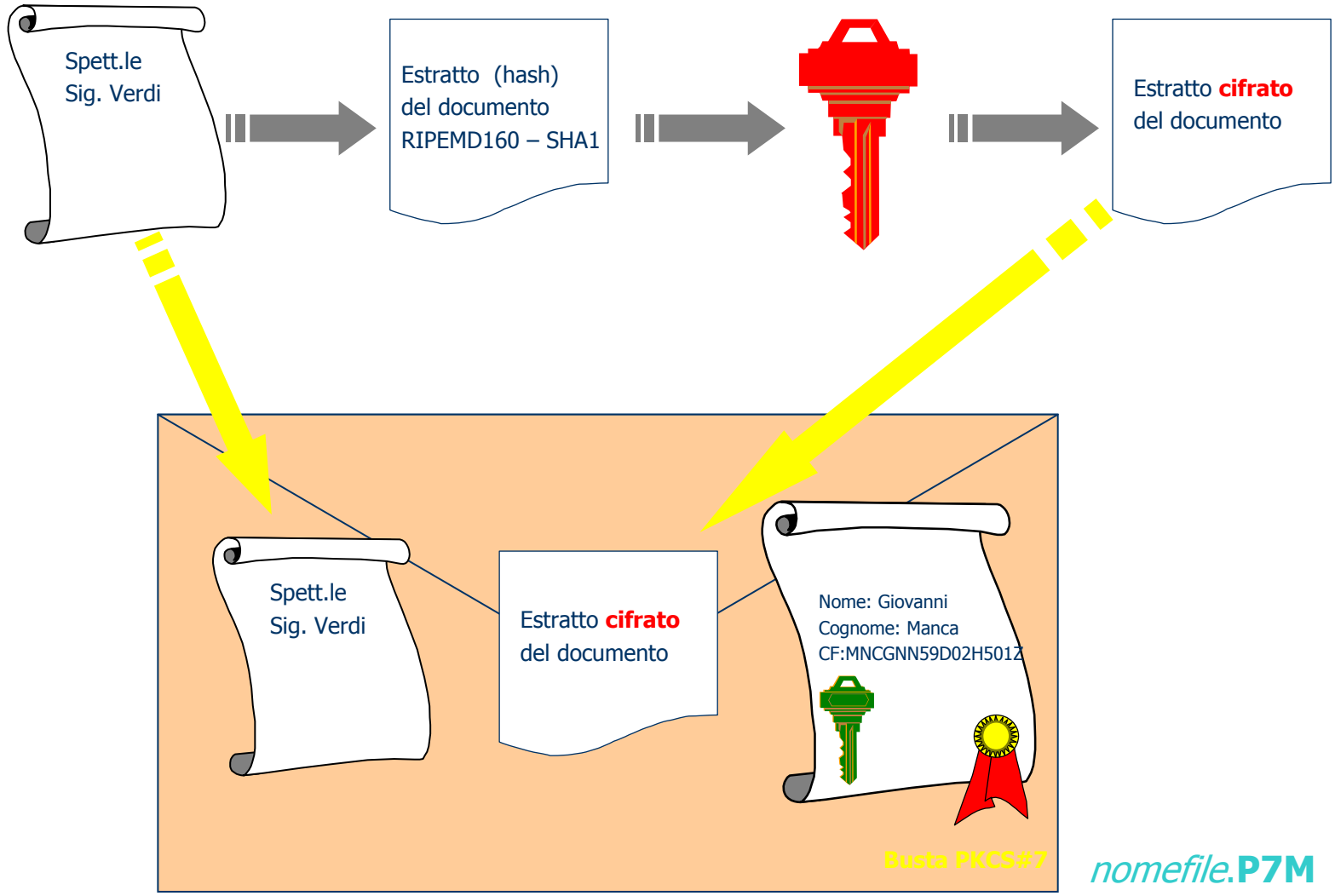
Inoltre resta da provare la possibilità di creare collisioni con due testi che rappresentino "atti o fatti giuridicamente rilevanti"

Hashing



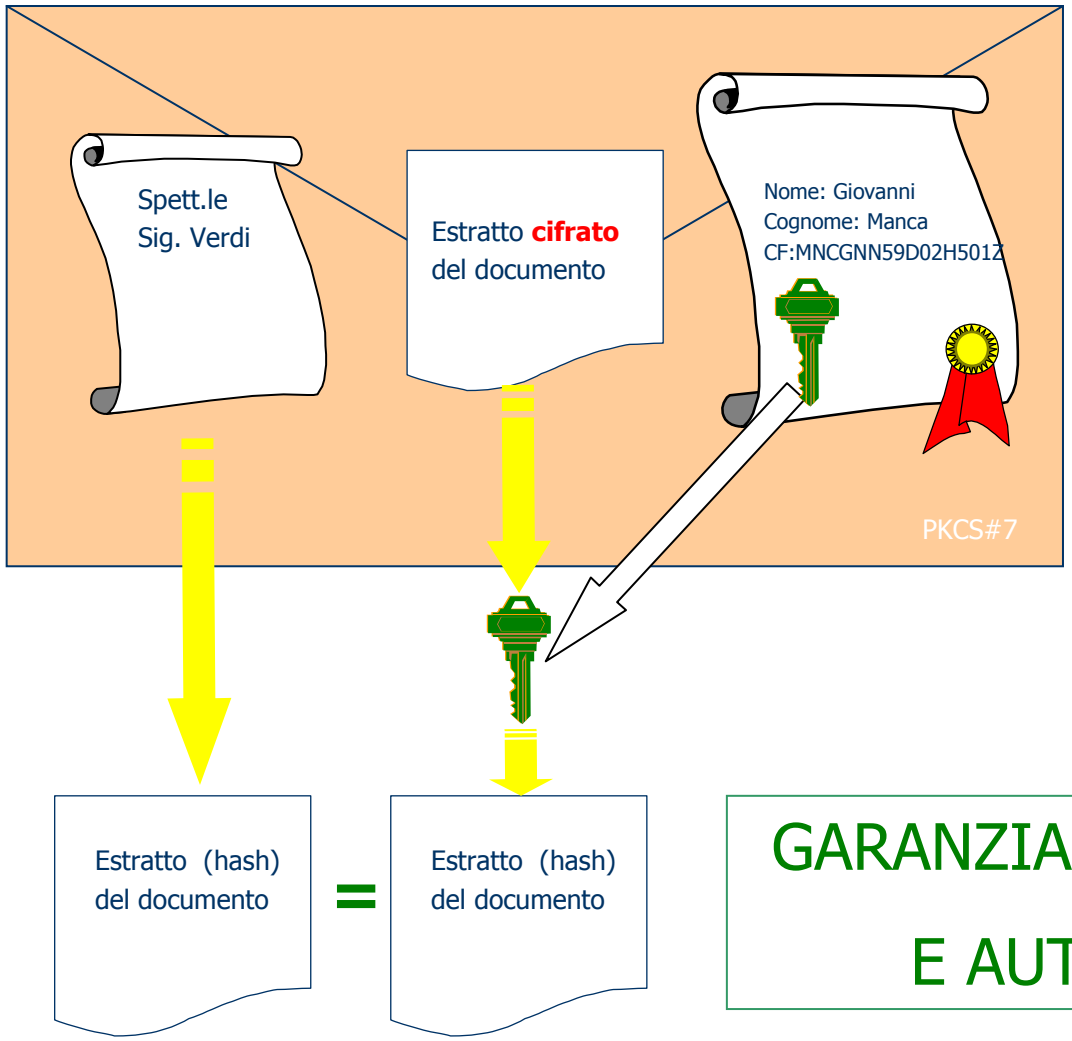
Digest: f(Mess.,Padd., I.V., Alg.)

La generazione della Firma



nomefile.**P7M**

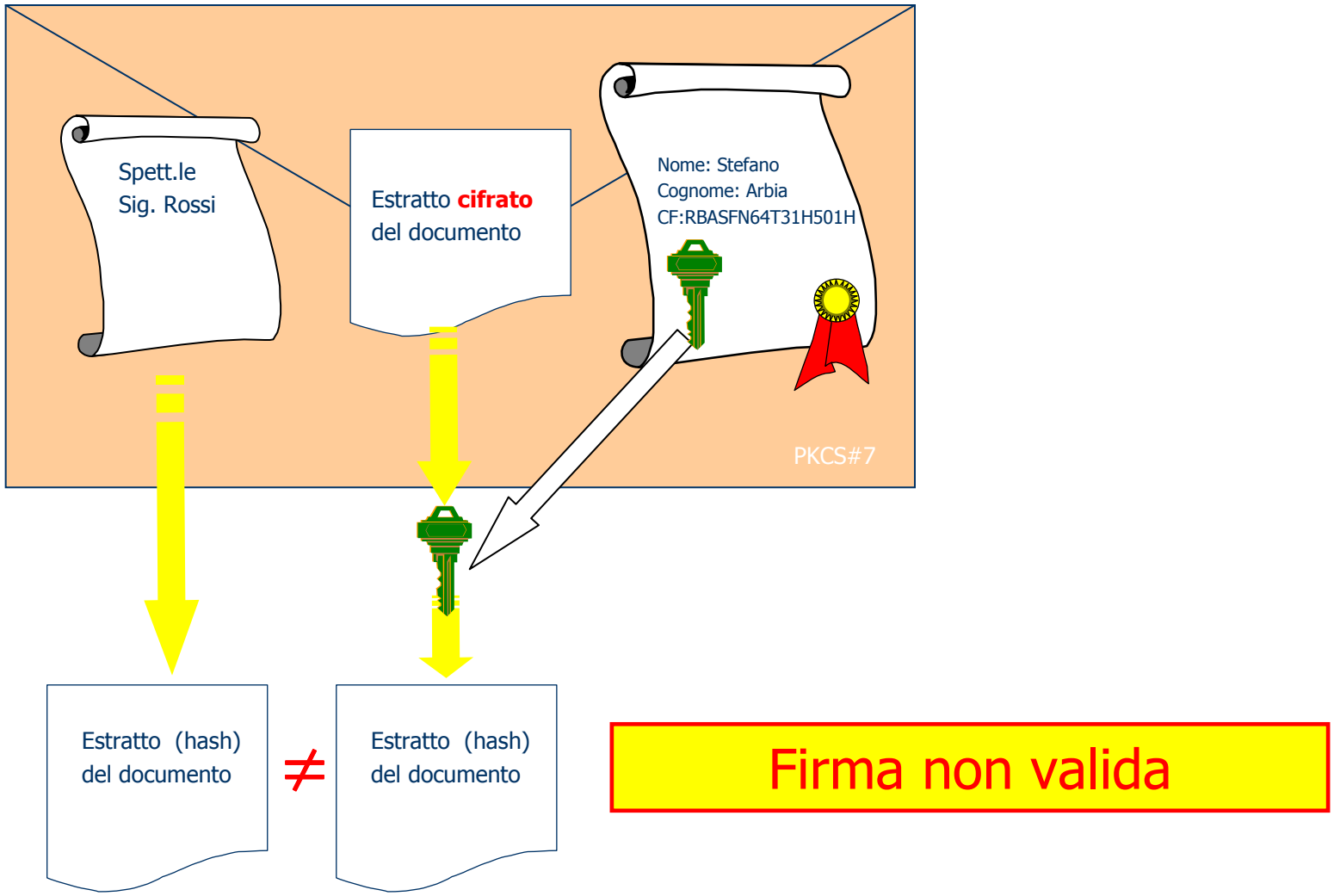
La verifica della firma digitale



GARANZIA DI INTEGRITA'

E AUTENTICITA'

La verifica della firma digitale



Il ruolo dei certificatori

Il ruolo dei certificatori

- Soggetti pubblici o privati che intendono rilasciare certificati qualificati
- I soggetti pubblici possono rilasciare certificati qualificati utili solo nei rapporti con l'Amministrazione stessa
- Se soggetti privati devono possedere requisiti societari particolari
- Tutti devono rispettare determinati requisiti tecnici, organizzativi, di sicurezza

Il ruolo dei certificatori

I certificatori accreditati rilasciano certificati qualificati utili per la firma digitale e certificati di autenticazione per le CNS

Nell'ambito del progetto CNS assumono un ruolo "strumentale", l'Ente Emettitore è sempre una PA

L'Elenco Pubblico dei Certificatori

Sul sito CNIPA **www.cnipa.gov.it** è disponibile l'Elenco Pubblico dei Certificatori Accreditati

Sottoscritto dal Presidente CNIPA a garanzia di autenticità e integrità

Pubblicato sul sito di tutti i certificatori accreditati

L'Elenco Pubblico dei Certificatori

Con Circolare CNIPA/CR/46, 27 gennaio 2005 (G.U. 4 febbraio 2005, n.28) sono stati pubblicati i codici identificativi della firma digitale del Presidente del CNIPA ai sensi dell'art. 41 del DPCM 13 gennaio 2004.

I codici in parola, costituiti dall'impronta del certificato della suddetta chiave pubblica, (omissis), sono i seguenti:

F758 2B22 3891 3258 A5F3 4FFF A06A 5A26 8997 732B, ottenuto utilizzando l'algoritmo (omissis), corrispondente alla funzione SHA-1.

Elenco dei certificatori europei

Elenco organismi di vigilanza e certificatori che emettono "certificati qualificati" in Europa disponibile sul sito EU-INFSO

http://europa.eu.int/information_society

http://europa.eu.int/information_society/eeurope/2005/all_about/security/esignatures/index_en.htm

L’importanza del tempo

- **Se un certificato viene revocato e non è possibile sapere se una certa firma è stata apposta quando esso era ancora valido, la firma è da “buttare”**
- **Ancora: dopo la scadenza di un certificato il certificatore non è tenuto a comunicarne eventuali revoche**

… quindi …

- **è indispensabile stabilire con certezza se la firma è stata creata prima della scadenza o revoca**

- **Attenzione: stabilire l’esistenza di un documento *prima* della firma non serve a nulla: chi ne garantisce autenticità e integrità prima della firma, se il certificato è revocato o scaduto?**

Le marche temporali

- **Dlgs 82/2005 (Codice) ART. 1.1**

  bb) *validazione temporale*, il risultato della procedura informatica, con cui si attribuisce, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi;

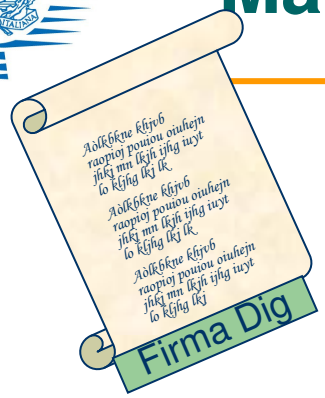
- **DPCM 13/1/2004, art. 1.1**

  i) *marca temporale*, un'evidenza informatica che consente la validazione temporale.

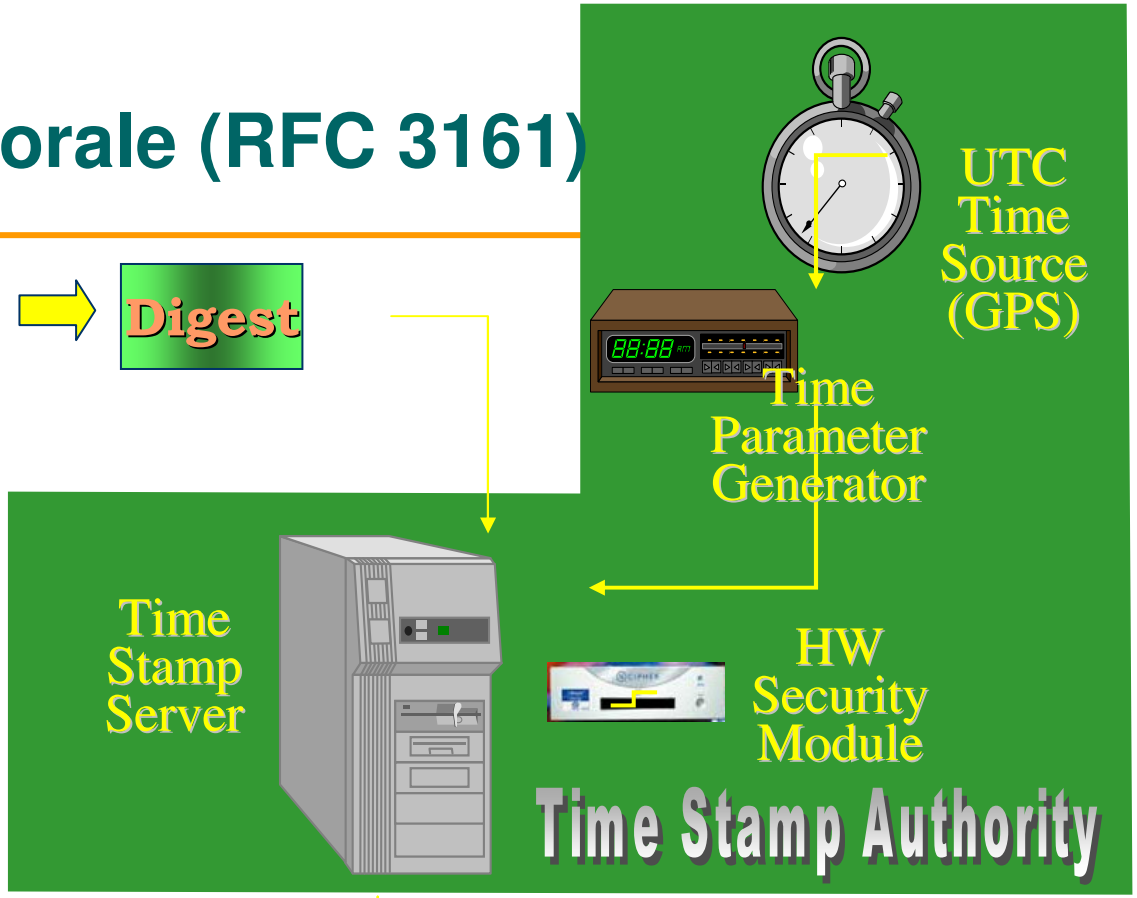
- **Una marca temporale è firmata da un ente affidabile (TSA) e contiene il riferimento univoco a un altro oggetto binario e l'indicazione certa del tempo.**

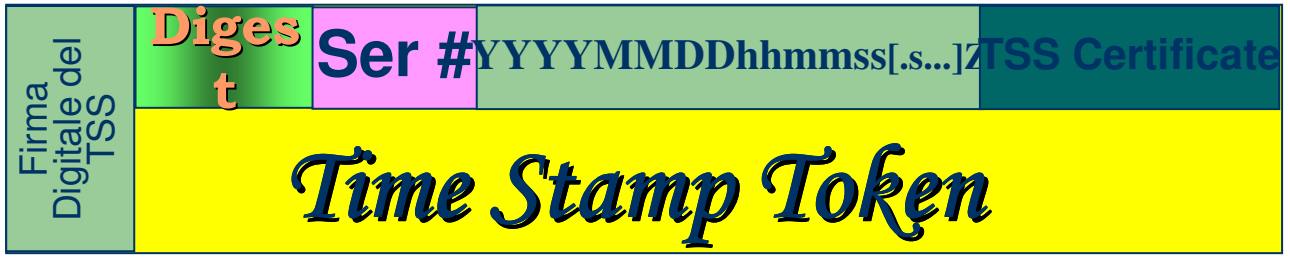
- ***Una marca temporale può in certi casi essere sostituita da un riferimento temporale affidabile: DPCM 13/1/2004*** ➔ ➔

Marca temporale (RFC 3161)



Hash → Digest





Riferimento temporale – DPCM 13/1/2004

- **Art. 1.1: g) *riferimento temporale*: informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici;**

- **Art. 39.4: Le pubbliche amministrazioni possono anche utilizzare come sistemi di validazione temporale:**
  a) **il riferimento temporale contenuto nella segnatura di protocollo …;**
  b) **il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti …;**
  c) **il riferimento temporale ottenuto attraverso l'utilizzo di posta certificata ….**

Qualche numero sulla diffusione

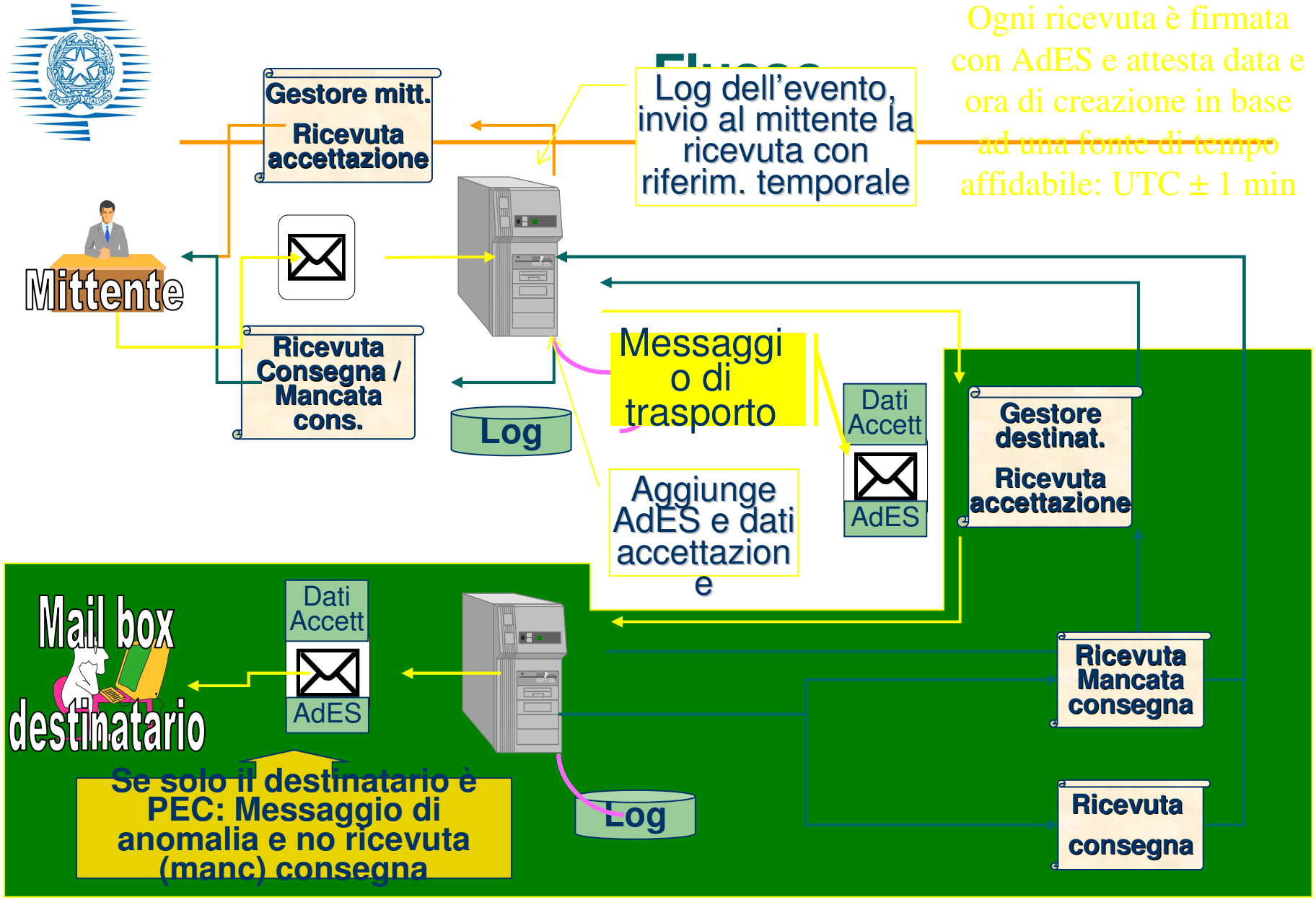
- **Attualmente l'elenco pubblico dei certificatori, disponibile sul sito del CNIPA è costituito da 18 soggetti;**
- **Ci sono circa 2.700.000 dispositivi di firma;**
- **Circa 40.000 nella pubblica amministrazione centrale;**
- **La Regione Lombardia sottoscrive e marca temporalmente circa 2,5 milioni di referti al mese.**
- **L'Arma dei Carabinieri ha dematerializzato completamente due procedimenti amministrativi**

Dematerializzazione

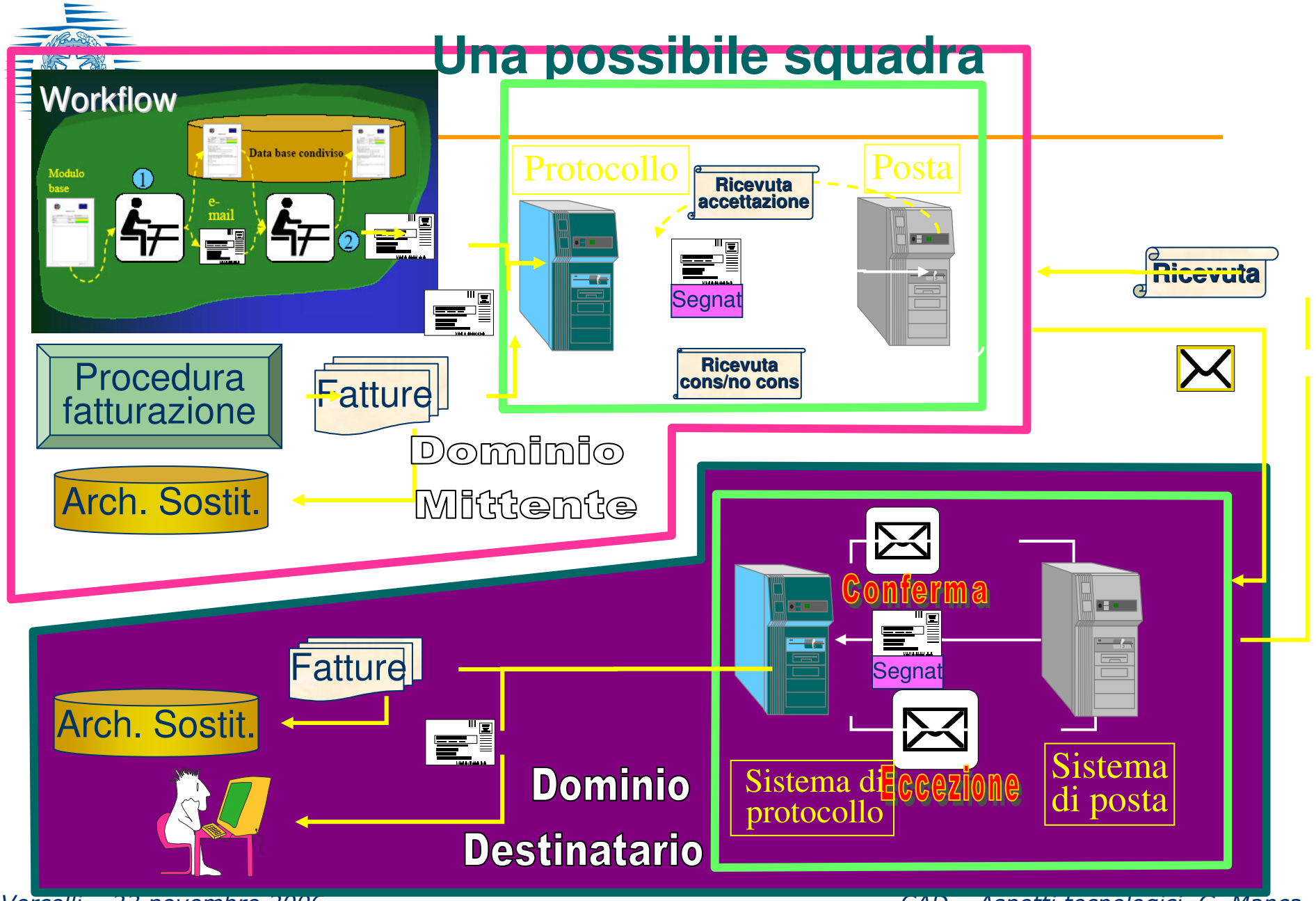
Art. 42 del Codice

- **“Le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle regole tecniche adottate ai sensi dell’articolo 71”.**

Un po’ di PEC

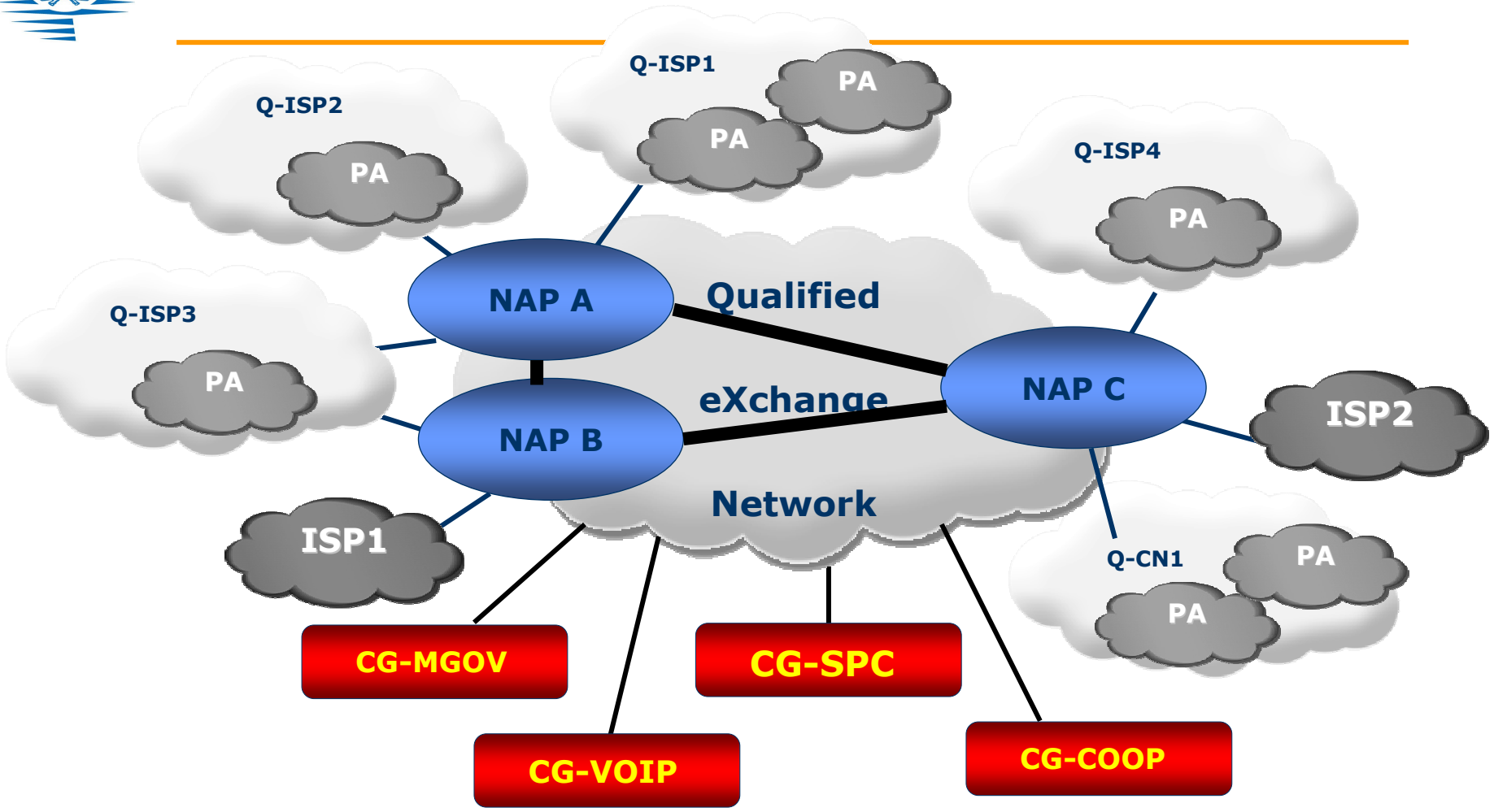

Gestore mitt.
Ricevuta accettazione
Log dell'evento, invio al mittente la ricevuta con riferim. temporale
Ogni ricevuta è firmata con AdES e attesta data e ora di creazione in base ad una fonte di tempo affidabile: UTC ± 1 min
Mittente
Ricevuta Consegna / Mancata cons.
Log
Messaggio di trasporto
Dati Accett
AdES
Gestore destinat.
Ricevuta accettazione
Aggiunge AdES e dati accettazione
Mail box destinatario
Dati Accett
AdES
Se solo il destinatario è PEC: Messaggio di anomalia e no ricevuta (manc) consegna
Log
Ricevuta Mancata consegna
Ricevuta consegna

Una possibile squadra



L’architettura del Sistema Pubblico di Connettività (SPC)

Architettura SPC



Sistema Pubblico di Connettività e Cooperazione

Per maggiori informazioni

www.cnipa.gov.it

manca@cnipa.it