UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

sistema PRAXIS

Servizi per l'e-government nell'università Federico II

La posta elettronica certificata, la firma digitale, i regolamenti di Ateneo

Napoli, 24 ottobre 2006

Elenco dei contenuti

sistema PRAXIS

I PARTE

Definizioni e concetti generali, cenni normativi

L'e-government: una definizione

Con il termine **e-government** si definiscono le **innovazioni di servizio e di processo** realizzate dalle **pubbliche amministrazioni** mediante l'utilizzo di Tecnologie dell'Informazione e della Comunicazione (**ICT**)

L'e-government: gli obiettivi

Le politiche di **e-government** promuovono la "**cultura dell'innovazione**" per conseguire i seguenti risultati:

- l'ottimizzazione delle attività interne alla PA;
- il miglioramento degli strumenti tradizionali nel rapporto tra le PA e tra i cittadini e le PA;
- la trasparenza dell'azione amministrativa;
- il potenziamento dei supporti conoscitivi per le decisioni pubbliche;
- il contenimento dei costi dell'azione amministrativa.

L'e-government ed il sistema PRAXIS

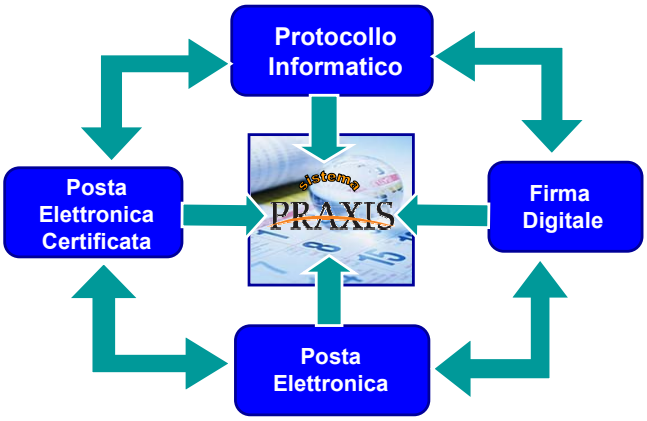
sistema PRAXIS

è l'insieme delle soluzioni tecnico-organizzative per l'e-government dell'Ateneo, in linea con la normativa vigente in materia di Amministrazione digitale.

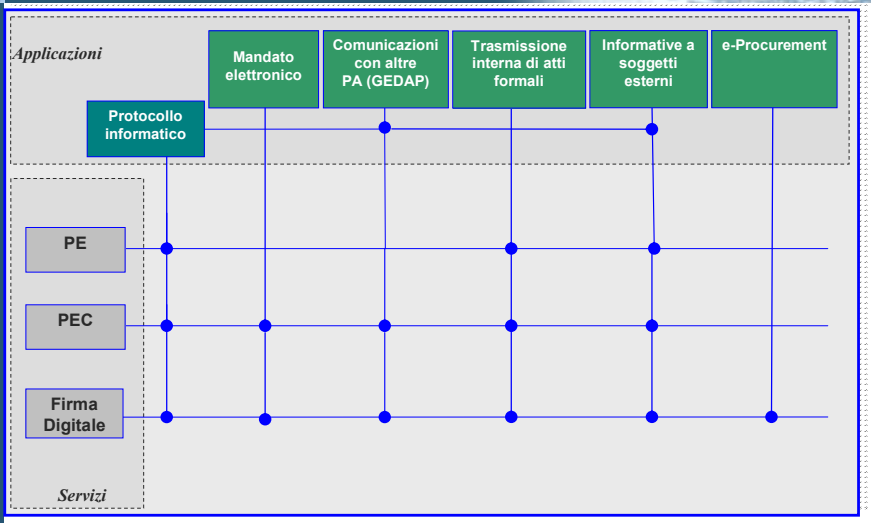
Il sistema **PRAXIS** si basa sull'utilizzo e sull'integrazione dei seguenti strumenti informatici:

- La Posta Elettronica (PE)
- La Posta Elettronica Certificata (PEC)
- La Firma Digitale
- Il Protocollo Informatico e la Gestione Documentale

Gli strumenti per l'e-Government



Le applicazioni ed i servizi per l'e-Government



Il Documento Informatico

- Le politiche di e-Government mirano alla dematerializzazione dei documenti cartacei, mediante la progressiva introduzione dei documenti informatici.
- Il "**documento informatico**" è definito come "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".
- Il 1° gennaio 2006 è entrato in vigore il D.lgs n.82/2005, denominato **Codice dell'Amministrazione Digitale** (**CAD**), strumentazione normativa coordinata con l'impianto giuridico vigente in materia di: formazione, gestione, riproduzione, conservazione, trasmissione ed accessibilità dei documenti informatici.

La normativa

- **Dlgs del 7 marzo 2005, n. 82 e succ. mod. (Dlgs 4.4.2006, n.159)**
  Codice dell'amministrazione digitale
- **DPR sulla PEC dell'11 febbraio 2005, n. 68**
  Regolamento recante disposizioni per l'utilizzo della PEC
- **Deliberazione CNIPA del 19 febbraio 2004, n. 11**
  Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali
- **DPCM 12 maggio 2005**
  Regole Tecniche per la formazione,la trasmissione e la validazione della PEC
- **DPCM del 13 gennaio 2004**
  Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici
- **DPR del 28 dicembre 2000, n. 445**
  Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
- **Direttiva europea 1999/93/CE del 13 dicembre 1999**
  Quadro comunitario per le firme elettroniche

La sicurezza del documento informatico

- L'utilizzo dei documenti informatici determina la necessità di stabilire regole e meccanismi informatici per garantire, in fase di formazione e di trasmissione:

  1. **Identità fisica del sottoscrittore**
  2. **Non-ripudio della paternità dei messaggi e degli allegati**
  3. **Riservatezza dello scambio**
  4. **Integrità dei documenti e degli allegati**
  5. **Affidabilità del circuito di trasporto**
  6. **Determinazione della data e dell'ora di formazione del documento o di trasmissione di un messaggio**
  7. **Identità dell'utente per l'accesso servizi in rete**

- In aggiunta, nuovi meccanismi informatici devono essere adottati per la conservazione sostitutiva dei documenti dematerializzati, per la riproduzione dei documenti su supporti non informatici, per l'archiviazione di documenti giuridicamante rilevanti.

La sicurezza digitale: funzionalità e soluzioni tecniche

Criticità	Funzionalità	Soluzione tecnica
• Identità fisica del Sottoscrittore	• Autenticazione	• Certificato qualificato
• Non-ripudio della paternità dei documenti e degli allegati	• Non ripudio	• Firma elettronica qualificata, oppure digitale
• Riservatezza dello scambio	• Confidenzialità	• Crittografia a chiave pubblica
• Integrità dei documenti e degli allegati	• Integrità dei dati	• Hashing
• Affidabilità del circuito di trasporto	• Ricevute qualificate	• Posta Elettronica Certificata
• Determinazione della data e dell'ora	• Marcatura temporale	• Time stamping
• Identità dell'utente per l'accesso servizi in rete	• Autenticazione	• Carta Nazionale dei Servizi

II PARTE

Posta Elettronica Certificata

La comunicazione dei documenti con strumenti informatici e telematici (1/2)

- L'art. 3 del CAD sancisce il principio generale in base al quale i cittadini e le imprese hanno il diritto di «richiedere» e di «ottenere» l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni centrali.
- Le comunicazioni telematiche o informatiche inviate da chiunque ad una pubblica amministrazione, con qualsiasi mezzo informatico o telematico idoneo a verificarne la provenienza, ivi compreso il fax, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale (CAD - art. 45.1).
- L'obbligo di comunicare per via telematica con i cittadini e le imprese che lo richiedano presuppone che l'amministrazione si adoperi per rendersi facilmente raggiungibile telematicamente; si rende, pertanto, necessario esporre ed evidenziare adeguatamente, sul sito istituzionale dell'amministrazione, gli indirizzi di posta elettronica utilizzabili dai cittadini, con l'indicazione di quelli abilitati alla posta elettronica certificata.

La comunicazione dei documenti con strumenti informatici e telematici (2/2)

- Il documento informatico trasmesso mediante **posta elettronica** si intende spedito dal mittente se è reso disponibile dal gestore del servizio di posta elettronica del destinatario all'indirizzo elettronico da questi dichiarato (CAD - art. 45.2).
- E' utile che le amministrazioni provvedano ad organizzarsi per realizzare servizi di informazione preventiva in modalità telematica, al fine di fornire tempestivamente, per posta elettronica, a coloro che lo abbiano esplicitamente richiesto, informazioni, documenti e notizie in merito a scadenze o a pagamenti da effettuare, moduli o formulari per richieste o eventuali rinnovi.
- Le amministrazioni dovranno evidenziare, comunque, che il cittadino e' tenuto ad assolvere i propri obblighi legati agli adempimenti scadenzati, a prescindere dall'effettiva ricezione della comunicazione.
- Viene fatto obbligo alle pubbliche amministrazioni di dotare ciascun dipendente di una casella di posta elettronica e di utilizzare la posta elettronica **entro il 1° settembre 2006** (CAD - art. 47.3) per le comunicazioni con i propri dipendenti.

La trasmissione dei documenti informatici tra pubbliche amministrazioni

- Le comunicazioni tra le pubbliche amministrazioni sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza (CAD - art. 47.1).
- Ai fini della verifica della provenienza, e comunicazioni sono valide se (CAD – art. 47.2):
  a) sono sottoscritte con **Firma Digitale** o altro tipo di firma elettronica qualificata;
  b) ovvero sono dotate di protocollo informatizzato;
  c) ovvero è possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'art. 71 del CAD;
  d) ovvero sono trasmesse via **Posta Elettronica Certificata**.

La posta elettronica certificata (PEC)

Definizione di PEC *(DPR n.68/2005, art. 1.2, lettera g))*

E' un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici

Un sistema di PEC:

- consente l'invio di messaggi la cui trasmissione è valida agli effetti di legge;
- gestisce i messaggi imbustati contenenti documenti primari ed allegati, eventualmente firmati;
- verifica la provenienza e l'avvenuta ricezione e consegna del messaggio;
- garantisce il controllo dell'integrità dei messaggi in fase di comunicazione tra diversi gestori e la registrazione della traccia delle operazioni svolte;
- implica, da parte del gestore del mittente, il controllo sulla presenza di virus informatici nel messaggio.

Il Codice dell'amministrazione digitale e la PEC

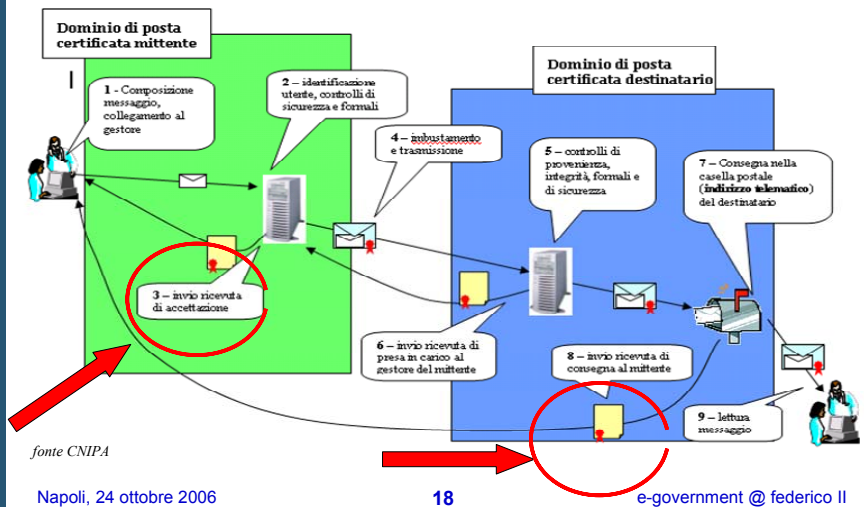
- Le pubbliche amministrazioni centrali (tra cui le istituzioni universitarie) sono tenute ad utilizzare la PEC per ogni scambio di informazioni e di documenti con i soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di PEC (CAD – art. 6.1). Questa volontà obbliga solo il dichiarante e può essere revocata nella stessa forma della dichiarazione;
- Inoltre, la PEC:
  - ✓ equivale alla notificazione via posta (raccomandata R/R) (CAD – art. 48.2);
  - ✓ garantisce autenticazione ed opponibilità ai terzi della data e l'ora di trasmissione e di ricezione di un documento informatico (CAD – art. 48.3);
  - ✓ deve ottemperare alla disciplina contenuta nel DPR 68/2005 (CAD – art. 48.1) "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata".

Entro il **1° settembre 2006** le pubbliche amministrazioni centrali sono tenute ad istituire almeno una casella di posta elettronica certificata, per ciascun registro di protocollo.

Caratteristiche generali del servizio PEC

- Il mittente o il destinatario che intendono fruire del servizio PEC si avvalgono dei gestori inclusi in un apposito elenco tento dal Centro nazionale per l'informatica della pubblica amministrazione (CNIPA).
- Tramite il gestore PEC l'utente mittente, utilizzando gli stessi client applicativi di posta elettronica comunemente adottati, invia il messaggio all'indirizzo di PEC del destinatario.
- Una volta inviato il messaggio, il server del gestore PEC provvede a fornire al mittente una ricevuta di accettazione sottoscritta mediante firma elettronica avanzata e ad inoltrare il messaggio al server di posta certificata del destinatario.
- Il gestore PEC del destinatario, a sua volta, provvede a fornire al mittente la ricevuta di avvenuta consegna del messaggio sulla casella di posta certificata del destinatario.
- L'interazione fra due distinti gestori, coinvolti nell'invio di un messaggio di posta certificata, è regolata dallo scambio di una ricevuta di presa in carico.
- Il gestore deve conservare il log delle trasmissioni effettuate per un periodo non inferiore ai 30 mesi.

La posta elettronica certificata: schema funzionale



fonte CNIPA

Raffronto PE-PEC

Strumento	Caratteristiche	Limiti	Ambito
Posta Elettronica	○ Ai fini del procedimento amministrativo, il documento/messaggio ○ scambiato tra PA ha validità solo se se è possibile accertarne la provenienza, quindi se è sottoscritto con firma digitale. ○ Con il cittadino, il documento trasmesso soddisfa il requisito della forma scritta, purché sia possibile accertarne la fonte di provenienza. ○ Il messaggio si intende inviato se trasmesso al proprio gestore, consegnato se reso disponibile all'indirizzo esplicitamente dichiarato dal destinatario.	Non si dispone, in modo giuridicamente valido di ricevute di invio e di consegna: dal punto di vista probatorio, è liberamente valutabile il log del sistema.	Informazione preventiva al cittadino- Documenti e comunicazioni ai dipendenti.
Posta Elettronica Certificata	○ La trasmissione ha validità. giuridica. Il documento trasmesso soddisfa il requisito della forma scritta ed è valida ai fini del procedimento amministrativo. ○ Equivale alla raccomandata R/R. ○ Autenticità, non ripudio, integrità in fase di trasmissione. ○ La data e l'ora della trasmissione sono opponibili ai terzi.	Devono essere dotati di PEC mittente e destinatario.	Documenti validi agli effetti di legge con altre PA o con soggetti privati, in sostituzione della posta con ricevuta di invio e di consegna.

La trasmissione di atti formali: diagrammi di flusso

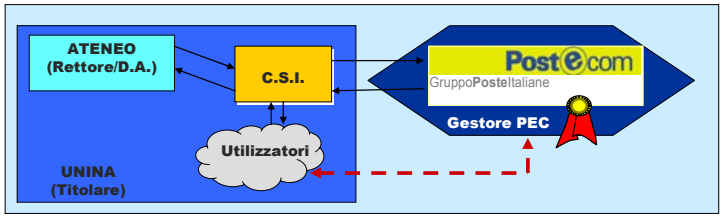
Il servizio PEC dell'Ateneo (1/2)

- L'Università ha istituito un proprio dominio di posta elettronica certificata, denominato «**pec.unina.it**», presso il gestore pubblico **Postecom S.p.A.**, ente iscritto nell'elenco dei gestori di PEC tenuto da CNIPA.
- L'Università nel suo complesso, il Rettorato, la Direzione Amministrativa, i Poli, le Facoltà, i Dipartimenti, i Centri di ricerca e di servizio interdipartimentali, nonché i Centri di Ateneo saranno dotati di una propria casella di posta elettronica certificata di capacità pari a 100 MB.
- Prima dell'avvio operativo del servizio risulta necessario definire le regole per:
  a. l'assegnazione, l'attivazione e la disattivazione degli indirizzi di PEC;
  b. la gestione delle credenziali di autenticazione ed autorizzazione all'utilizzo del servizio;
  c. le modalità operative per l'amministrazione del dominio pec.unina.it;
  d. il coordinamento dell'utilizzo della PEC con la firma digitale ed il protocollo informatico;
  e. le finalità di utilizzo interno all'Ateneo della PEC.

Il servizio PEC dell'Ateneo (2/2)

C.S.I. (Centro Servizi Informativi d'Ateneo) è il responsabile dell'amministrazione del dominio pec.unina.it e, pertanto, svolge le seguenti attività:

- definizione dei nuovi indirizzi PEC di ciascuna struttura,
- attivazione/disattivazione delle caselle,
- interfaccia tecnica verso il Gestore PEC,
- supporto di I e II livello agli utenti,
- monitoraggio del raggiungimento della soglia prefissata di occupazione delle caselle di PEC.



III PARTE

Firma Digitale

Le firme informatiche

LE FIRME INFORMATICHE
(D.Lgs. 82/2005, art. 1)

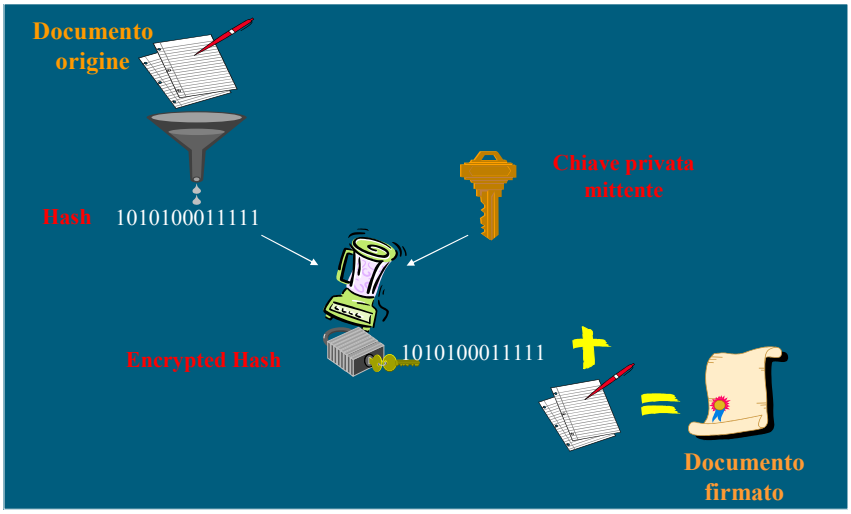
Firma elettronica (D.Lgs. 82/2005, art. 1.1, lettera q)	Firma elettronica qualificata (D.Lgs. 82/2005, art. 1.1, lettera r)	Firma digitale (D.Lgs. 82/2005, art. 1.1, lettera s)
l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica.	la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato.	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.

La firma digitale - Generalità

- La firma digitale è basata su un procedimento di "crittografia asimmetrica" che fa uso di una **coppia di chiavi** a 1024 bit: 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, l'Ente Certificatore, riconosciuto da CNIPA.
- Per ogni Titolare, il Certificatore crea una coppia di chiavi asimmetriche.
- Il Certificatore, per ciasun Titolare, genera e consegna al richiedente un **dispositivo sicuro di firma** contenente: la coppia di chiavi assieme ad un certificato di firma che consente l'associazione della persona con la sua chiave pubblica.

  Oltre alla **identificazione e registrazione** certa del richiedente, l'Ente Certificatore ha anche il compito di gestire l'intero ciclo di vita del certificato, compresa la sospensione temporanea della sua validità o la sua revoca definitiva.

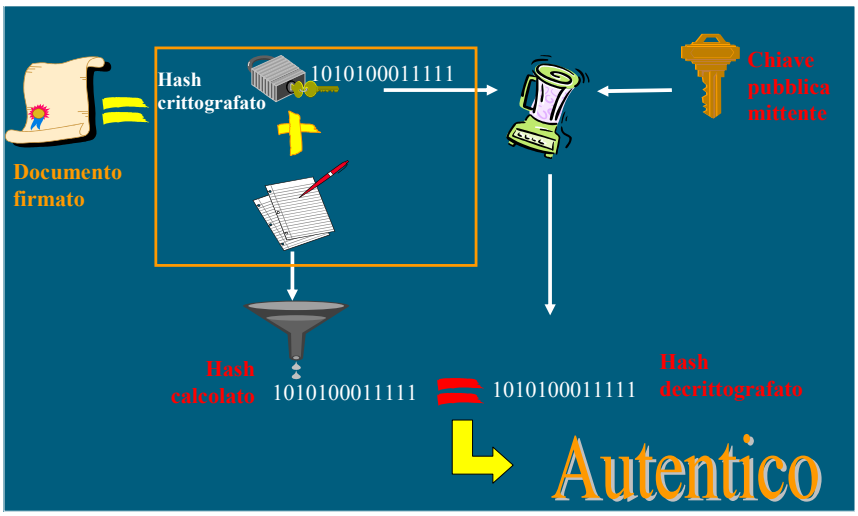
Il processo di firma



L'impronta del documento e le funzioni di hash

- Una funzione di hash H effettua una trasformazione di un messaggio m che riceve in input generando come output un messaggio h=H(m) di lunghezza fissa e ridotta rispetto a quella di m
- Le funzioni di hash utilizzate in crittografia soddisfano le seguenti proprietà:
  - il messaggio m in ingresso può essere di qualsiasi lunghezza
  - il messaggio h in uscita ha sempre lunghezza fissa
  - la computazione h=H(m) è veloce e poco onerosa
  - la trasformazione H(m) è monodirezionale (one-way)
  - la probabilità di collisione della funzione H(m) è quasi nulla
- Nell'ambito del processo di firma digitale di un documento informatico, la normativa prevede l'uso della funzione di hash ISO/IEC SHA-1 che produce un'impronta di lunghezza pari a 160 bit.

La verifica della firma digitale



Il certificato qualificato ed il formato di firma

- La chiave pubblica, insieme ai dati necessari per identificare il sottoscrittore della firma elettronica qualificata o digitale, è contenuta nel certificato qualificato.
- Tale attestato elettronico è rilasciato da certificatori qualificati, cioè soggetti che prestano servizi di certificazione delle firme elettroniche e che dimostrano, inoltre, adeguata affidabilità organizzativa, tecnica e finanziaria per svolgere attività di certificazione.
- I certificatori qualificati in possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza, chiedono di essere accreditati presso il CNIPA.
- Il documento da firmare è imbustato nel formato originale, senza aggiunte in testa o in coda al formato stesso. Il nome del file firmato, ossia della busta, assume l'ulteriore estensione «p7m» ed aggrega al suo interno:
  - **il documento informatico nel formato originale,**
  - **la firma elettronica qualificata o digitale ad esso associata,**
  - **il certificato qualificato del sottoscrittore.**

Il Codice dell'amministrazione digitale e la firma digitale

- Il documento informatico sottoscritto con **firma digitale** (oppure, elettronica qualificata):
  - soddisfa il requisito legale della forma scritta (CAD – art. 20.2),
  - ha efficacia giuridico-probatoria (CAD – art. 21.2),
  - garantisce autenticazione, non ripudio (fino a querela di falso da parte del sottoscrittore) ed integrità,
  - l'uso della firma digitale integra e sostituisce ad ogni fine di legge l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti (CAD – art. 24.2).
- Il documento informatico a cui è apposta una **firma elettronica**:
  - è liberamente valutabile sotto il profilo probatorio (CAD – art. 21.1).
- Le pubbliche amministrazioni possono rivolgersi a **certificatori accreditati** (CAD – art. 34.1, comma b)).

Il Codice dell'amministrazione digitale ed il certificato qualificato (1/2)

- I certificati qualificati (CAD – art. 28.1) devono contenere almeno le seguenti informazioni:
  a) indicazione che il certificato elettronico rilasciato è un certificato qualificato;
  b) numero di serie o altro codice identificativo del certificato;
  c) nome, ragione o denominazione sociale del certificatore che ha rilasciato il certificato e lo Stato nel quale è stabilito;
  d) nome, cognome o uno pseudonimo chiaramente identificato come tale e codice fiscale del titolare del certificato;
  e) dati per la verifica della firma, cioè i dati peculiari, come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica corrispondenti ai dati per la creazione della stessa in possesso del titolare;
  f) indicazione del termine iniziale e finale del periodo di validità del certificato;
  g) firma elettronica qualificata del certificatore che ha rilasciato il certificato.

Il Codice dell'amministrazione digitale ed il certificato qualificato (2/2)

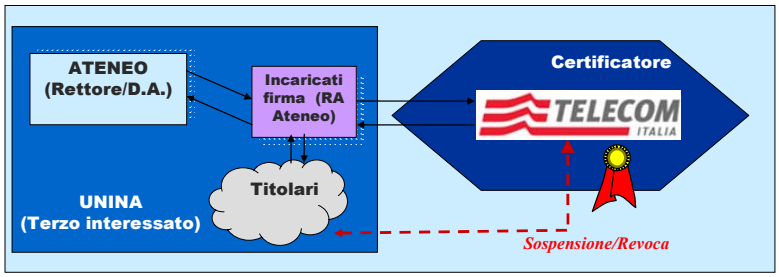
- Il certificato qualificato (CAD – art. 28.3) può contenere, ove richiesto dal titolare o dal terzo interessato, le seguenti informazioni:
  a) le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;
  b) limiti d'uso del certificato;
  c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili.
- L'emissione di un certificato qualificato può essere richiesta, oltre che dal titolare, anche da un soggetto "terzo interessato" (CAD – art. 28.3).
- Il certificatore raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso (CAD – art. 32.5).
- Il certificatore è obbligato a tenere registrazione di tutte le informazioni relative al certificato qualificato dal momento della sua emissione per almeno 20 anni (CAD – art. 32.3, comma j)).

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

- E' il servizio per la gestione della distribuzione dei certificati qualificati per la **firma digitale**.
- L'Ateneo, in qualità di "terzo interessato", si avvale dei servizi offerti dal **certificatore accreditato IT Telecom S.r.l.**.
- Si basa sulla organizzazione di una "Registration Authority" interna, costituita da amministrativi dell'Ateneo all'uopo incaricati dalla Direzione Amministrativa, delegati dal certificatore.
- I certificati qualificati ed i dispositivi sicuri di firma, costituiti da "token USB" contenenti la chiave crittografica di sottoscrizione ed il certificato del titolare, saranno assegnati ai responsabili di struttura, secondo le indicazioni fornite dal Rettore e dal Direttore Amministrativo.
- La firma digitale, integrata nell'architettura funzionale e di servizio dell'e-government, sarà utilizzata nell'ambito del protocollo informatico e dell'e-procurement.

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

- L'avvio del nuovo servizio necessita della definizione di:
  - ✓ **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) nei confronti del Certificatore, e degli Interessati/Titolari,**
  - ✓ **diritti dell'Ateneo, in qualità di "terzo interessato".**



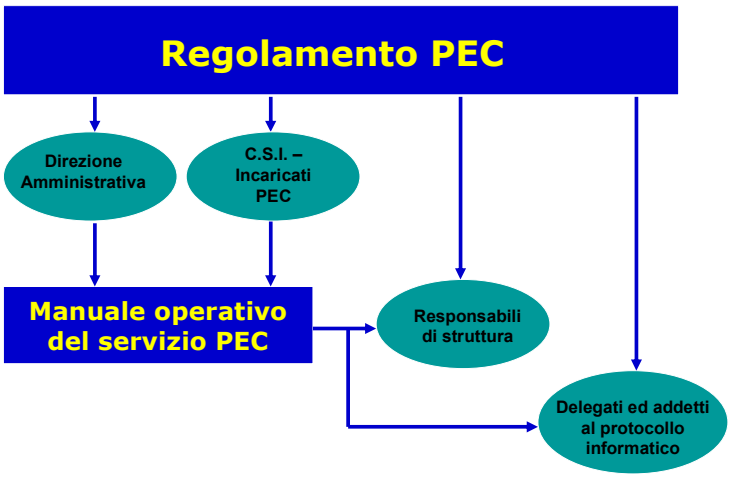
IV PARTE

I regolamenti d'Ateneo in materia di posta elettronica certificata e di firma digitale

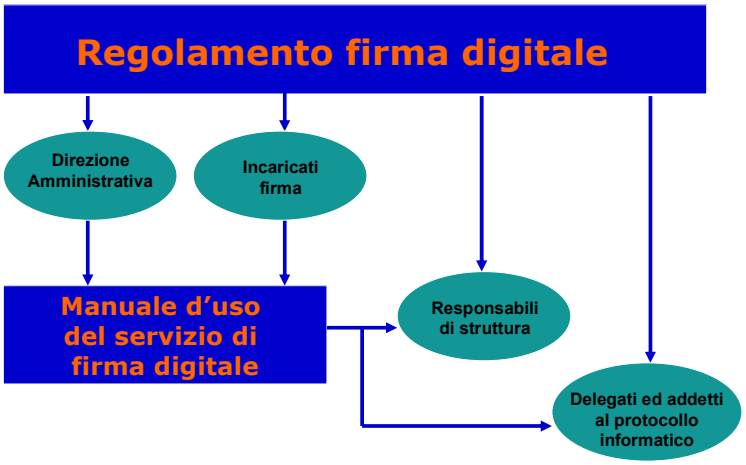
Finalità dei regolamenti per la PEC e la firma digitale

- ✓ Fornire il quadro di riferimento normativo in materia di PEC e di firma digitale.
- ✓ Definire l'ambito di utilizzo di tali strumenti nella gestione dei documenti di rilevanza amministrativa.
- ✓ Coordinarne l'impiego con quello di altri strumenti a supporto dell'e-government quali, ad esempio, il protocollo informatico.
- ✓ Individuare le categorie dei soggetti interessati e stabilire le regole per l'attivazione o la disattivazione di caselle PEC, oppure, l'assegnazione, la sospensione o la revoca dei certificati, nel rispetto della tutela dei dati personali.
- ✓ Organizzare l'erogazione del servizio d PEC e di firma digitale, in termini di: strutture funzionali coinvolte, iter delle informazioni, modalità di interfaccia con il gestore/certificatore.
- ✓ Definire gli obblighi e le responsabilità degli attori coinvolti nell'intero processo.

Utilizzatori del regolamento PEC



Utilizzatori del regolamento firma digitale



Struttura del regolamento in materia di PEC

- Introduzione:
  - oggetto, finalità del regolamento ed ambito di applicazione del servizio
  - definizioni generali
  - i ruoli coinvolti
- Descrizione dei ruoli:
  - compiti degli incaricati_PEC
  - obblighi dell'utente_PEC
- Elementi per la gestione del servizio:
  - caratterizzazione delle diverse tipologie di caselle PEC
  - creazione e cessazione delle caselle PEC
  - attivazione e disattivazione dell'utente_PEC
- Norme di coordinamento con il D.Lgs 196/2003 in materia di protezione dei dati personali
- Disposizioni finali

Struttura del regolamento in materia di firma digitale

- Introduzione:
  - oggetto, finalità del regolamento ed ambito di applicazione del servizio
  - definizioni generali
  - i ruoli coinvolti
- Descrizione dei ruoli:
  - obblighi del certificatore e del titolare
  - compiti e responsabilità degli incaricati_firma
- Elementi per la gestione del servizio:
  - circostanze per la revoca o per la sospensione dei certificati
  - regole operative per l'uso della firma digitale in Ateneo
- Norme di coordinamento con il D.Lgs 196/2003 in materia di protezione dei dati personali
- Disposizioni finali

Redatto da Clelia Baldo – clelia.baldo@unina.it

Stampato dal Centro Stampa di Ateneo