Firma digitale, HTTPS, SPID, PEC e Protocollo informatico

Angela Peduto

Università degli Studi di Salerno, *20/09/20212*

1

Indice degli argomenti

- Contesto: trasformazione digitale
- *Strumenti per la dematerializzazione:*
  - *HTTP e HTTPS*
  - *Firma digitale*
  - *Protocollo informatico*
  - *Prosta eletrronica certificata*
  - *SPID*

2

Trasformazione digitale

- L'emergenza Covid ha fornito un'occasione importante per accelerare il processo di digitalizzazione anche per la PA.
- il 2020 è stato caratterizzato da importanti provvedimenti del Governo – contenuti nei Decreti "Cura Italia", "Rilancio", "Semplificazioni" – per accelerare l'innovazione.
- il digitale e le reti di collaborazione hanno consentito agli enti locali di resistere all'emergenza, continuando a garantire i servizi essenziali, raggiungere e sostenere la popolazione più colpita.

Dott. ssa Angela Peduto - anpeduto@unisa.it

3

Alcuni dati

- con il decreto Cura Italia per la prima volta in gran parte delle amministrazioni pubbliche si è passati al lavoro agile
- dal sondaggio del Forum PA di maggio 2020 è emerso come per l'87,7% degli enti pubblici sia stata la prima volta.
- bilancio positivo:
  - l'88% dei dipendenti ha giudicato l'esperienza di successo,
  - il 69,5% ha potuto programmare meglio il lavoro,
  - il 34,9% ha lavorato in un clima di maggior fiducia e responsabilizzazione
  - per il 41,3% dei dipendenti pubblici, l'efficacia lavorativa è migliorata.

Dott. ssa Angela Peduto - anpeduto@unisa.it

4

Dematerializzazione

- Con il termine dematerializzazione si vuole indicare pertanto, il progressivo incremento della gestione documentale informatizzata all'interno della Pubblica Amministrazione e la sostituzione dei supporti tradizionali della documentazione amministrativa in favore del documento informatico.
- Obiettivi:
  - si adottano criteri per evitare o ridurre in maniera significativa la creazione di nuovi documenti cartacei;
  - si punta ad eliminare i documenti cartacei attualmente esistenti negli archivi, sostituendoli con opportune registrazioni informatiche e scartando la documentazione non soggetta a tutela per il suo interesse storico-culturale.

5

Strumenti per la trasformazione digitale

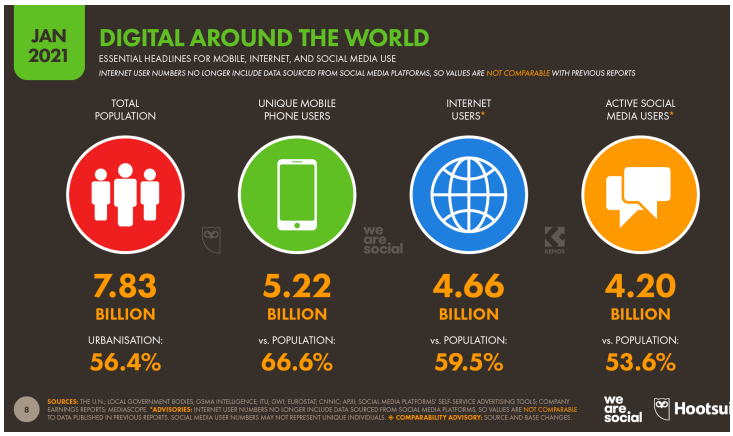
"C'è vero progresso solo quando i vantaggi di una nuova tecnologia diventano per tutti."

H. Ford

6

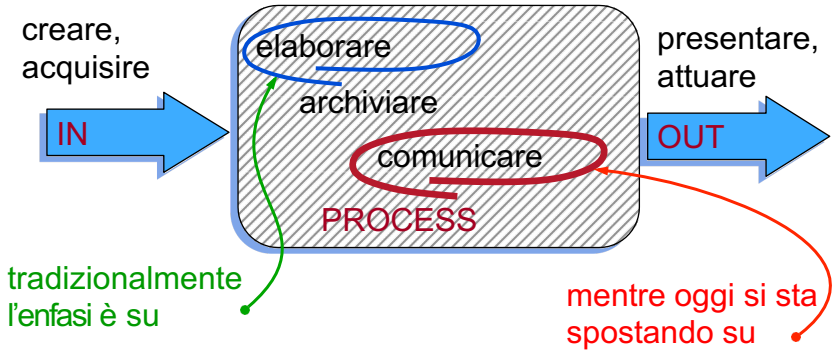
La diffusione di internet

- Sono quasi **4,66 miliardi le persone** che oggi sono **connesse a internet** con un incremento del 1,8% (dal 2019 al 2020 era del 9% circa).
- più del **60% della popolazione mondiale è online**



7

Reti di comunicazione



… cioè sull'interconnessione in rete dei sistemi di elaborazione …

8

Perche la rete?

- Condividere risorse
  - utilizzo razionale di risorse HW (magari costose)
  - Condivisione di software (programmi e dati da parte di utenti)
  - affidabilità e disponibilità delle risorse
- Comunicare tra utenti
  - scambio informazioni
  - collaborazione a distanza

9

Cos'è una rete

Una rete informatica è un insieme di dispositivi collegati tra loro tramite sistemi di interconnessione (cablaggio o wireless).

10 m	stanza	Rete locale LAN
100 m	edificio	LAN
1 km	università	LAN
10 km	città	Rete metropolitana MAN
100 km	nazione	Rete geografica WAN
1000 km	continente	Internet
10000 km	pianeta	Internet

10

Rete di computer

- Ogni elaboratore collegato a una rete viene detto ***nodo*** o host.
- I dati trasmessi vengono raggruppati in ***pacchetti*** per essere trasmessi e ricevuti da un host all'altro.
- Il pacchetto (frame) rappresenta una quantità di dati di dimensione standardizzata, che può variare secondo il ***protocollo di comunicazione*** utilizzato.

11

I protocolli di comunicazione

- Per comunicare i calcolatori debbono seguire delle le ***regole***: i protocolli di comunicazione.
- I protocolli di comunicazione specificano:
  - i formati dei dati
  - la struttura dei pacchetti
  - la velocità di trasmissione
- – …

12

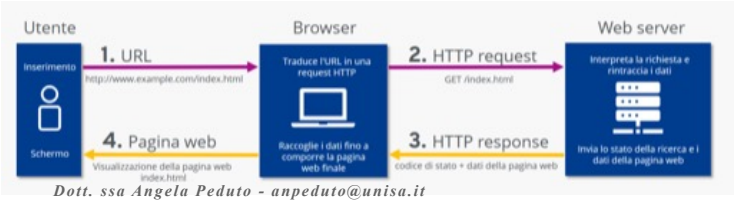
Alcuni protocolli applicativi

- HTTP
  - Per navigare sul web
- HTTPS
  - Per acquistare su web in modo sicuro
- SMTP
  - Per spedire email
- POP
  - Per ricevere email e scaricarle sul proprio PC
    - Una volta scaricate sul PC le email non sono leggibili con altri dispositivi ma non serve più essere collegati a internet per consultarle
- IMAP
  - Per ricevere email senza scaricarle sul proprio PC
    - La mail può essere letta da qualunque dispositivo ma bisogna essere collegati a internet

13

Cos'è l'HTTP?

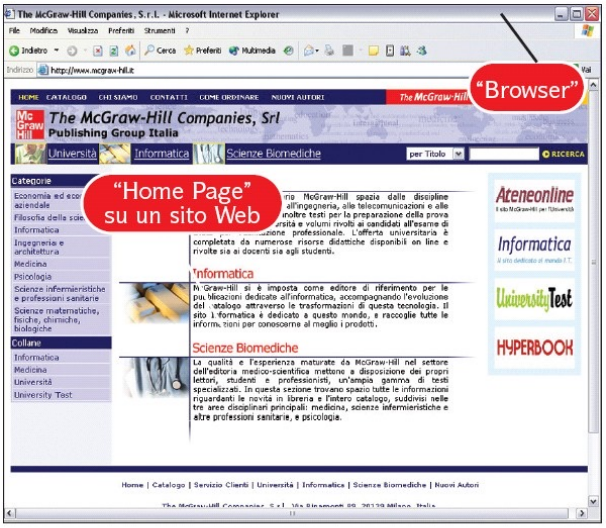
- HTTP è l'abbreviazione di protocollo di trasferimento ipertestuale.
- Le pagine Web vengono archiviate su server, che vengono quindi servite al computer client quando l'utente vi accede.
- La rete risultante di queste connessioni crea il world wide web come lo conosciamo oggi.
- Senza HTTP, il world wide web (WWW) per come lo intendiamo non esisterebbe.



14

Un pagina Web

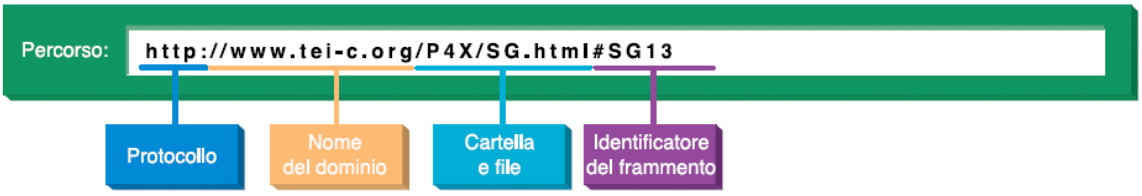
- Ciò che appare all'utente sul suo schermo è l'unione di due elementi ben diversi: il **browser**, l'applicazione che consente di navigare tra le pagine web, e il **contenuto** di una pagina presente su un sito.



Home page del sito della McGraw-Hill Italia
http://www.mcgraw-hill.it

Analisi di un indirizzo web (URL)

- Ogni parte dell'URL identifica, sempre più specificatamente, la posizione dell'elemento.



Indirizzo IP

- Un Indirizzo IP è un numero (a 32 bit) che identifica univocamente i dispositivi collegati con una rete informatica che utilizza lo standard IP (Internet Protocol)
  - – Ciascun dispositivo (router, computer, server di rete, stampanti, alcuni tipi di telefoni, ...) ha il suo indirizzo.

17

Indirizzi IP e DNS

L'IP ***non è di semplice comprensione*** da parte dell'utente, ed è quindi uso comune assegnare ad ogni IP un ***nome simbolico***

Per fare questo si utilizza il ***Domain Name System (DNS)***, che associa uno o più nomi ad ogni IP, e gestisce la conversione tra le due codifiche.

IP	DNS	Nome simbolico
157.27.6.235	⟷	www.univr.it

18

Problema

Con una connessione HTTP:

- i dati trasferiti non sono crittografati, quindi si corre il rischio che malintenzionati rubino le informazioni che vengono trasmesse.

19

Una definizione rapida di HTTPS

- HTTPS sta per protocollo di trasferimento ipertestuale sicuro ed è la versione crittografata di HTTP.
- Viene usato per comunicazioni sicure su Internet o su una rete.
- Il protocollo di comunicazione è crittografato utilizzando Transport Layer Security (TLS) o, in precedenza, Secure Sockets Layer (SSL).

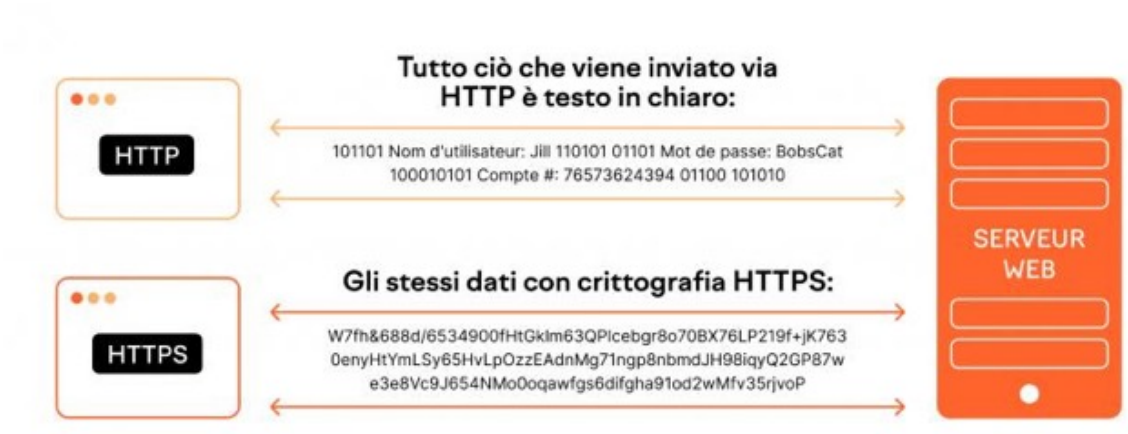
20

Come funziona HTTPS?

- A differenza di HTTP, HTTPS usa un certificato di protezione di un fornitore terzo per rendere sicura una connessione e verificare che il sito sia legittimo.
- Questo certificato di sicurezza è noto come certificato SSL.
- SSL è l'abbreviazione di "secure sockets layer".
- Questo certificato crittografa una connessione con un livello di protezione definito al momento dell'acquisto del certificato SSL.

21

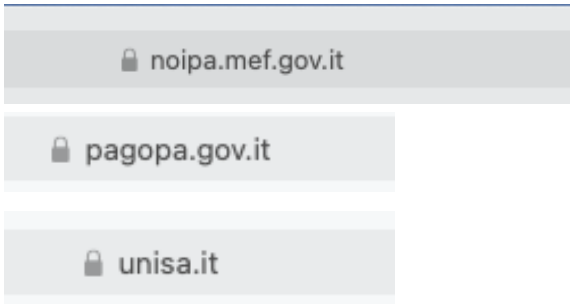
HTTP VS HTTPS



23

Riconoscere un sito che usa https

- https://noipa.mef.gov.it/cl/it/web/guest/home
- https://www.pagopa.gov.it
- https://www.unisa.it



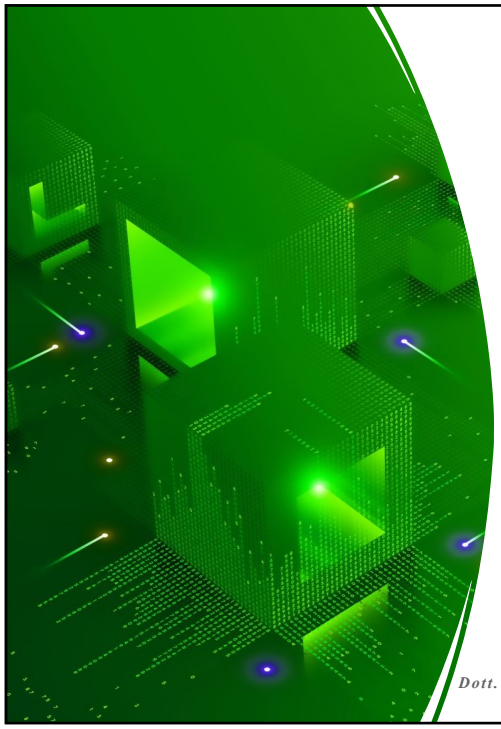
24

La sicurezza in rete

Le quattro principali aree in ambito di sicurezza in rete sono:

- *segretezza dei dati*
- *autenticazione*
- *firme elettroniche*
- *controllo di integrità*

25



La crittografia

- La crittografia è l'arte di progettare algoritmi (o cifrari) per crittografare un messaggio rendendolo incomprensibile a tutti tranne al suo destinatario
- Il destinatario, con un algoritmo simile deve essere in grado di codificarlo, attraverso un parametro segreto detto chiave (usato in precedenza anche dal mittente per la cifratura)

26

Algoritmo di crittografia

- Un algoritmo di crittografia riceve un testo da codificare (detto testo in chiaro) e lo trasforma, attraverso la ***chiave***, in un testo cifrato apparentemente incomprensibile

27

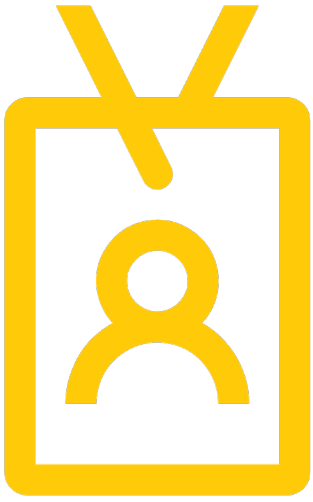
I dati cifrati sono inviolabili?

- La crittografia risulta necessaria ovunque si voglia archiviare o trasmettere dati riservati, rendendo impossibile (o meglio molto difficile) l'accesso a chi non dispone della chiave

28

La firma digitale

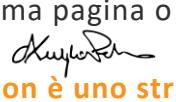
- La firma digitale viene da molti considerata uno dei migliori mezzi possibili per ridurre drasticamente i problemi di sicurezza relativi alla trasmissione di documenti per via telematica



29

Cosa non è la firma digitale

- La firma digitale **non è l'immagine digitalizzata della propria firma autografa** posizionata, automaticamente dal software, sulla prima pagina o alla fine di un documento.



- La firma digitale **non è uno strumento di crittografia** dei documenti elettronici.

30

Firma digitale

La firma digitale è il risultato di una procedura informatica che garantisce l'autenticità e integrità

dei messaggi e documenti scambiati e archiviati con mezzi informatici,

al pari della firma autografa per i documenti tradizionali.

Dott. ssa Angela Peduto - anpeduto@unisa.it

31

Firme

- Spesso si parla di firma elettronica e firma digitale utilizzandole come sinonimi, senza capirne le differenze e il relativo valore probatorio.
- Occorre fare un po' di chiarezza.
- Vediamo nel dettaglio le diverse tipologie di firme previste dal Codice dell'Amministrazione Digitale e le differenze a livello legale.

32

Firma elettronica

33

Firma elettronica

- Partendo dalla definizione contenuta nel regolamento *(dati elettronici connessi ad altri)* una firma elettronica può essere implementata in modo piuttosto semplice

Credenziali di autenticazione:

User Id + Password

E' una prima forma semplice di firma elettronica, utilizzata in numerose applicazioni informatiche

Ad esempio **le credenziali di accesso ad un dato sito web,** come nome utente e password.

34

User Id Password

Sistema sicuro?

- Lunghezza e composizione delle password
- Stessa password per N servizi .. Visibile a chi gestisce il servizio?
  - Nei sistemi informatici attuali è buona norma conservare l'hash delle password
- Dove «conservare» le password

Username	PWD (SHA 256)
admin	7146084e6f06271dc0c85182476244f2b2d4f0f8fcc9e0dc9c250b83cce9ceb0
Felice Russo	ef797c8118f02dfb649607dd5d3f8c7623048c9c063d532cc95c5ed7a898a64f
Marco Indomabile	008be6875298f5a65763851b274e87055f3101a9c0477e583813c187cba187e6

35

Firma elettronica

- Sul **piano legale**, il valore probatorio di un documento dotato di semplice firma elettronica non è certo a priori e anzi **spetta al giudice valutarne le caratteristiche** oggettive di qualità, sicurezza, integrità e immodificabilità.

  La firma elettronica è quindi intrinsecamente debole tanto che in molti frangenti può essere liberamente giudicabile.

- La **firma elettronica semplice non** riesce ad **assicurare** i tre fondamentali obiettivi che le altre tipologie di firma elettronica perseguono, ossia **l'autenticità, il non ripudio e l'integrità del documento**

Dott. ssa Angela Peduto- anpeduto@unisa.it

37

FEA
Firma Elettronica Avanzata

Dott. ssa Angela Peduto- anpeduto@unisa.it
Dott. ssa Angela Peduto - anpeduto@unisa.it

38

Firma elettronica avanzata

Secondo il regolamento eIDAS per ***Firma elettronica avanzata*** si intende una firma elettronica che soddisfi i seguenti requisiti:

a) è connessa unicamente al firmatario;

b) è idonea a identificare il firmatario;

c) è creata 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;

- firma grafometrica, viene apposta su tablet ed è molto diffusa nel settore bancario e nel settore assicurativo
- prende in considerazione alcuni **parametri biometrici** derivanti dal gesto di apposizione ed acquisiti dal dispositivo sul quale è apposta, fra i quali rientrano ad esempio la posizione del pennino, la velocità, il ritmo e la pressione di scrittura.

39

Limiti della FEA

- La **FEA** incontra però dei limiti. L'art. 21 del CAD specifica che tale tipologia di firma non può essere utilizzata per la sottoscrizione degli atti indicati all'art. 1350 c.c., numeri da 1 a 12, per i quali il legislatore richiede necessariamente una firma elettronica di più alto livello (FEQ).
- Quest'ultima tipologia di firma, oltre a non incontrare i limiti previsti invece per la FEA, **risulta essere dal punto di vista legale la scelta più idonea** alla sottoscrizione dei documenti elettronici, con particolare riferimento a quelli aventi contenuto patrimoniale.

40

FEQ
Firma Elettronica Qualificata

Dott. ssa Angela Peduto - anpeduto@unisa.it

41

Firma elettronica qualificata

La ***Firma elettronica qualificata*** è una particolare firma elettronica avanzata basata su un **certificato qualificato** e realizzata mediante un **dispositivo sicuro** **che soddisfi i** requisiti dell'allegato II del regolamento eIDAS

[Definizione Art. 1,c. 11, eIDEAS]

La firma elettronica qualificata garantisce in modo univoco l'identificazione del titolare, e, dal punto di vista dell'efficacia giuridica, equivale ad una firma autografa, come statuito dall'art. 25 del Regolamento eIDAS.

E' una tipologia di firma superiore alla FEA, non può essere rilasciata da chiunque ma solo da certificatori qualificati

Dott. ssa Angela Peduto - anpeduto@unisa.it

42

Certificato – validità e revoca

a) Il periodo di validità è determinato dal certificatore (anche sulla base della robustezza delle chiavi utilizzate)
b) I certificati possono essere revocati o sospesi (su richiesta del titolare o dello stesso certificatore)
c) La revoca o sospensione ha effetto dal momento della pubblicazione.

Pubblicazione dove? Liste pubbliche

a) Lista dei certificati sospesi CSL
b) Lista dei certificati revocati CRL

Il certificatore deve tenere registrazione, di tutte le informazioni relative ad un certificato qualificato **per almeno 20 anni dalla sua emissione** elettronica,

Dott. ssa Angela Peduto - anpeduto@unisa.it

44

Certificatori – Prestatore di servizi fiduciari qualificati

- La lista dei prestatori di servizi fiduciari qualificati è presente nel sito AGID https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia
- Il certificatore rilascia un **certificato elettronico**. Cioè:

«un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona».

[Art. 3,c. 14, eIDAS]

Dott. ssa Angela Peduto- anpeduto@unisa.it
Dott. ssa Angela Peduto - anpeduto@unisa.it

45

Firma elettronica qualificata

Firma elettronica qualificata: è una particolare firma elettronica avanzata basata su un **certificato qualificato** e realizzata mediante un **dispositivo sicuro** per la creazione della firma

Tali **dispositivi** consistono in supporti elettronici rimovibili (smart card, chiavetta USB, token), che consentono al loro titolare di sottoscrivere un documento informatico, apponendovi la propria firma elettronica qualificata.

Se è su smart card si dovrà scaricare ed istallare un software sul pc se è su chiavetta USB il software è nella chiavetta baserà inseirire la chiavetta.

Firma digitale

La **firma digitale** **è una peculiare tipologia di firma elettronica qualificata**, prevista solamente a livello nazionale

Art 1, c. 1, lett s) CAD Firma digitale:

«Un particolare tipo di firma elettronica qualificata basata su un certificato qualificato e 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 o di un insieme di documenti informatici»

Dott. ssa Angela Peduto - anpeduto@unisa.it

Firma autografa e digitale

- La **firma autografa** è direttamente riconducibile all'identità di colui che la appone mediante il riconoscimento della **calligrafia**;
- la **firma digitale** non ha questa caratteristica per cui si ricorre all'**autorità di certificazione**, il cui compito è quello di stabilire, garantire e pubblicare l'associazione tra un soggetto e le firme digitali da lui generate.
- Questa associazione viene formalizzata tramite un **certificato** elettronico.

Garanzie della firma digitale

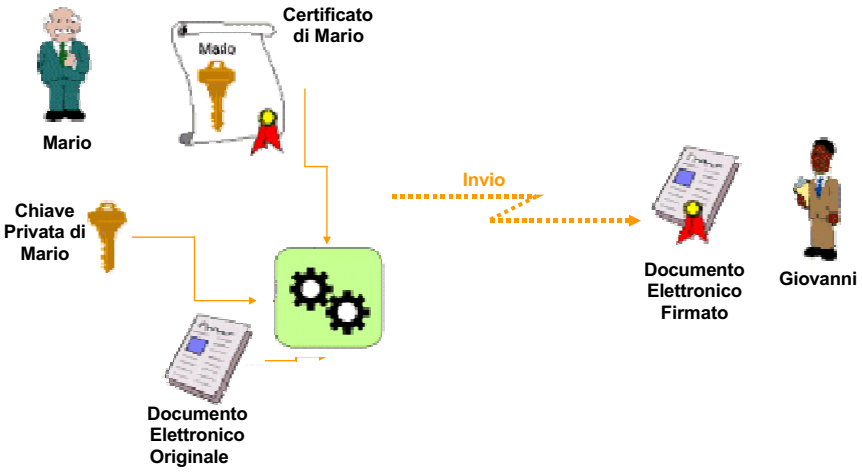
- L'associazione tra documento e firma autografa è ottenuta esclusivamente attraverso il supporto cartaceo;
- la firma digitale è invece **legata al singolo documento elettronico** a cui è apposta;
- a documenti elettronici diversi corrispondono **firme digitali diverse**;
- è **impossibile trasferire una firma digitale** da un documento ad un altro.

La firma di un documento

- Per firmare un documento elettronico occorre un software rilasciato da un'autorità di certificazione;
- La firma viene generata seguendo questi passi:
  - **generazione dell'impronta** a partire dal documento elettronico;
  - **generazione della firma mediante cifratura dell'impronta**;
  - **apposizione della firma** al documento elettronico e generazione della **busta crittografica**.

51

Schema



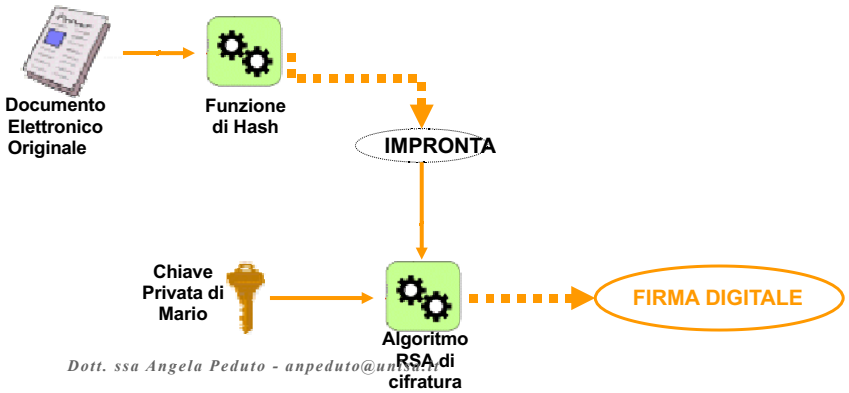
52

impronta

- Al documento da firmare viene applicata una particolare funzione (*funzione di hash*) che produce, una **sequenza binaria di lunghezza costante** chiamata impronta;
- la funzione garantisce che **a testi diversi non corrisponde la stessa impronta**;
- dall'impronta **è impossibile risalire al documento** originale.

generazione della firma

- Con la **chiave privata** del sottoscrittore, contenuta nella SmartCard e segreta a chiunque, **l'impronta viene cifrata**, ottenendo così una sequenza binaria che corrisponde alla **firma digitale.**

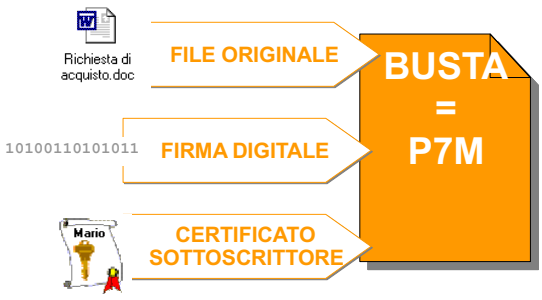


apposizione della firma

- La firma digitale viene **aggiunta alla fine del documento elettronico**;
- insieme con la firma viene **allegato anche il certificato del sottoscrittore**.
- il **certificato contiene la chiave pubblica** necessaria per la verifica dell'autenticità e dell'integrità del documento.

55

Schema di dettaglio



56

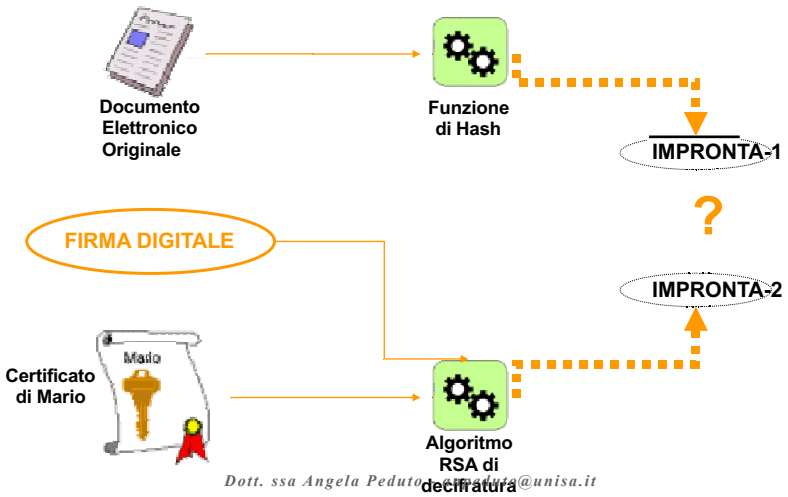
Formato di una firma digitale

Firme multiple
o Firme apposte allo stesso documento da vari sottoscrittori

Dott. ssa Angela Peduto - anpeduto@unisa.it

57

La verifica del documento firmato



59

Firma digitale remota

- **Cos'è la firma digitale remota? È diversa dalla firma digitale?**
- La firma digitale remota è un sistema che usa un App installata sullo smartphone o su un tablet e quindi non richiede ne un lettore ne una porta usb
- Si collega via internet ad un server nel quale sono conservati i certificati di firma di quel soggetto.
- La firma apposta con questo sistema è la stessa che si appone con le smart card o i token-chiavetta e quindi su questo fronte non ci sono differenze;
- tuttavia presenta alcuni limiti:
  - richiede sempre una connessione attiva;
  - non è user fiendly quindi poco si addice ad un uso massivo e frequente

60

Firma digitale remota (esempio cont.)

- L'attivazione del certificato è la prima operazione che si deve effettuare per poter rendere utilizzabile il Certificato e poter effettuare le operazioni di firma remota.
- Dalla pagina principale del Portale scegliere l'opzione "OTP VIA CELLULARE" e premere "INVIA OTP"
- Sul numero di cellulare indicato al momento della registrazione arriverà un SMS contenente il codice OTP richiesto.
- Dal menu scegliere quindi l'opzione "RICHIEDI CERTIFICATO" .

61

Sistema di gestione dei procedimenti amministrativi nazionali (SGPA)

Piattaforma per la digitalizzazione, i processi di dematerializzazione e la conservazione

62

Sistema di gestione dei procedimenti amministrativi nazionali (SGPA)

- Il Sistema di gestione dei procedimenti amministrativi nazionali (SGPA) rappresenta una delle piattaforme essenziali per il raggiungimento degli obiettivi di digitalizzazione, di semplificazione e di efficientamento dell'azione amministrativa della Pubblica Amministrazione previsti dall'Agenda digitale italiana e dal CAD.
- Il sistema ha l'obiettivo di garantire l'uniformità e l'interoperabilità a livello nazionale dei flussi documentali associati ai procedimenti amministrativi.

63

Il protocollo elettronico

Strumenti connessi alla piattaforma SGPA

64

L'attività di protocollazione

- l'operazione con la quale si memorizzano le informazioni principali relative al documento nel registro di protocollo,
- è quella fase del processo amministrativo che **certifica provenienza e data di acquisizione del documento identificandolo in maniera univoca** per mezzo dell'apposizione di informazioni numeriche e temporali.
- le pubbliche amministrazioni, ai sensi del Decreto Legislativo 30 marzo 2001, n. 165 art.1 comma 2, sono tenute a realizzare la gestior protocollo con sistemi informativi automatizzati

Dott. ssa Angela Peduto - anpeduto@unisa.it

65

Il protocollo informatico - definizione

- Il registro informatico di protocollo, unico per tutto l'ente, si apre il 1° Gennaio e si chiude il 31 Dicembre di ogni anno.
- Il servizio del protocollo informatico prevede:
  - Un **ufficio** apposito che provveda ad erogare il Servizio di protocollo informatico
  - Un dirigente o un funzionario, detto **Responsabile del servizio**, in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita e lavorerà in sinergia con il Responsabile dell'ufficio "archivio";

66

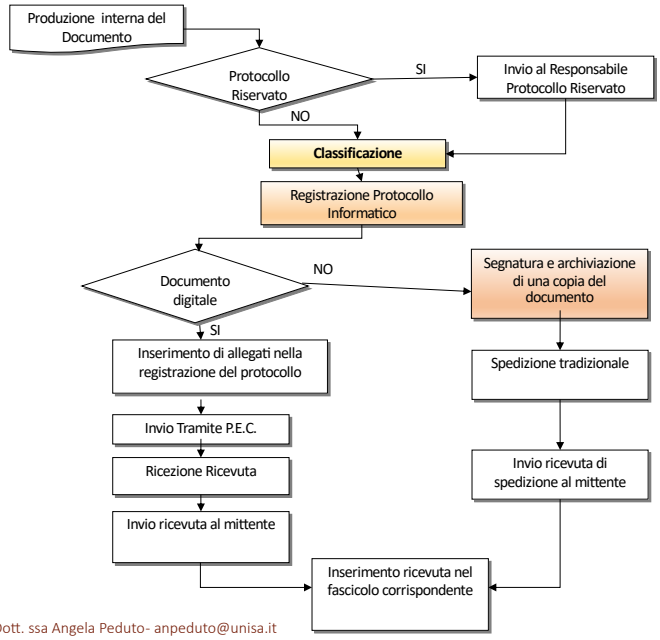
Il protocollo informatico - operazioni (nucleo minimo)

Per la corretta tenuta del protocollo informatico sono necessarie e sufficienti le seguenti operazioni:

- **Classificazione**: si attribuisce il documento a un titolo, una classe ed eventualmente un fascicolo in conformità al **titolario di classificazione** adottato.
- **Registrazione** Protocollo: inserendo i seguenti dati non modificabili:
  - numero di protocollo
  - data di registrazione
  - Mittente /destinatario o destinatari
  - oggetto del documento
  - data e protocollo del documento ricevuto, se disponibili;
  - l'impronta del documento informatico, se trasmesso per via telematica, generato automaticamente dal sistema e registrato in forma non modificabile;
- **Segnatura** è l'apposizione o l'associazione all'originale del documento, in forma permanente, non modificabile, delle informazioni riguardanti il documento stesso.

67

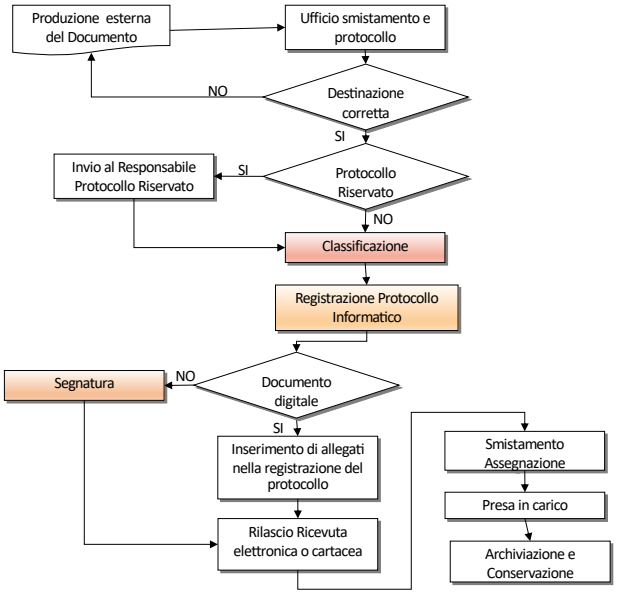
Il protocollo informatico- Schema flusso documenti in uscita



Dott. ssa Angela Peduto- anpeduto@unisa.it

68

Il protocollo informatico - Schema flusso documenti in ingresso



Dott. ssa Angela Peduto- anpeduto@unisa.it

69

Classificazione e Fascicolazione

- Mediante le operazioni di classificazione e registrazione di protocollo vengono attribuiti a ciascun documento **dei codici di riferimento** che lo identificano e lo associano agli altri documenti che formano la stessa pratica, nell'ambito di una delle serie di un determinato archivio.

70

Linee guida AgID

- Il primo gennaio 2022 sono divenute definitivamente efficaci le **Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici,** come previsto nella proroga inserita nella determinazione n. 371/2021 del 17 maggio 2021.
- https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_sul_documento_informatico.pdf

71

Sistema Pubblico per la gestione dell'Identità Digitale - SPID

72

Cos'è SPID

SPID è il sistema di autenticazione che permette a cittadini ed imprese di accedere con un'identità digitale unica a tutti i servizi online della Pubblica Amministrazione.

L'identità SPID è costituita da **credenziali** (nome utente e password) che vengono rilasciate all'utente e che permettono l'accesso ai servizi online.

spid Sistema Pubblico di Identità Digitale

73

Decreto semplificazione n. 76/2020 convertito in legge 120/2020

Indicazioni di semplificazione e innovazione digitale stabilite a livello nazionale:

- **pagamenti** per importi dovuti alla Pubblica Amministrazione dovranno essere effettuati attraverso la modalità PagoPA, con alcune eccezioni per le quali non è necessaria (F24, domiciliazione bancaria SDD, pagamenti per cassa).
- l'**autenticazione** per l'accesso ai servizi della Pubblica Amministrazione dovrà avvenire **esclusivamente tramite l'identità digitale SPID**, oppure utilizzando **CIE** Carta d'Identità Elettronica o **CNS** Carta Nazionale dei Servizi (Tessera sanitaria)

SPID - Identity Provider

Soggetti coinvolti:

- **Identity Provider – Gestori di identità**

Soggetti accreditati presso AgID che attribuiscono l'identità digitale a chi lo richiede. Forniscono le credenziali e permettono la verifica delle credenziali ai Service Provider

Tali soggetti, secondo l'art. 64 del CAD, devono soddisfare i requisiti di cui art.24 regolamento eIDAS
(Requisiti per i prestatori di servizi fiduciari qualificati)

https://www.spid.gov.it/richiedi-spid

SPID - Service Provider

Soggetti coinvolti:

- **Service Provider – Fornitori di servizi**

Fornitori di servizi (privati o PA) che utilizzano SPID per gestire l'accesso ai propri servizi.
Il fornitori si servizi inviano le richieste di identificazione agli Identity Provider e ricevono un esito positivo o negativo

https://web.unisa.it/servizi-on-line/spid

SPID
Adesione delle PA

art. 14 DPCM 24 ottobre 2014

- Le pubbliche amministrazioni possono affidare ai gestori di identità SPID le funzioni di autenticazione informatica basate sugli strumenti per i quali il diritto dell'Unione europea prevede il mutuo riconoscimento.

- Le pubbliche amministrazioni, in qualità di fornitori dei servizi, usufruiscono gratuitamente delle verifiche rese disponibili dai gestori di identità ' digitali e dai gestori di attributi qualificati. Per l'adeguamento allo SPID dei propri sistemi informatici, le amministrazioni utilizzano le risorse finanziarie disponibili a legislazione vigente, senza nuovi e maggiori oneri a carico della finanza pubblica..

SPID
Gestione identità digitali

Principali regole nella gestione delle identità digitali (art. 8 DPCM 24 ottobre 2014):

- gli utenti sono obbligati a informare tempestivamente il gestore dell'identità digitale di ogni variazione degli attributi previamente comunicati. Il gestore dell'identità digitale provvede tempestivamente ai necessari aggiornamenti, avendo verificato le informazioni fornite
- l'utente può chiedere al gestore dell'identità digitale, in qualsiasi momento e a titolo gratuito, la sospensione o revoca della propria identità digitale ovvero la modifica dei propri attributi secondari e delle proprie credenziali di accesso

81

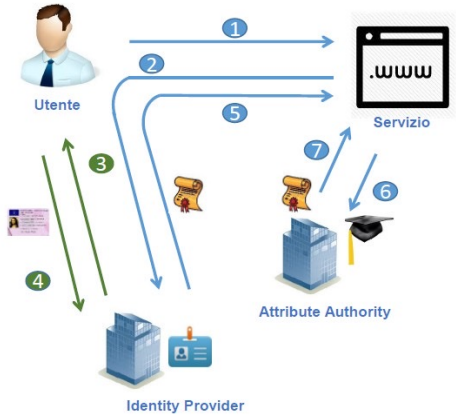
SPID
Gestione identità digitali

In caso di uso illecito delle identità digitali (art. 9 DPCM 24 ottobre 2014):

- Nel caso in cui l'utente ritenga, ... , che la propria identità digitale sia stata utilizzata abusivamente o fraudolentemente da un terzo, può chiedere, con le modalità indicate nei regolamenti di cui all'art. 4, la sospensione immediata dell'identità digitale al gestore della stessa e, se conosciuto, al fornitore di servizi presso il quale essa risulta essere stata utilizzata
- La sospensione ha una durata massima di 30 giorni, dopo di questa l'identità è ripristinata o revocata

82

SPID
Schema funzionamento



1. Richiesta di servizio
2. Inoltro verso Identity provider
3. Richiesta credenziali
4. Verifica credenziali
5. Rendirizzamento verso il service provider con asserzione di autenticazione
6. Richiesta attributi
7. Risposta contenente certificazione attributi

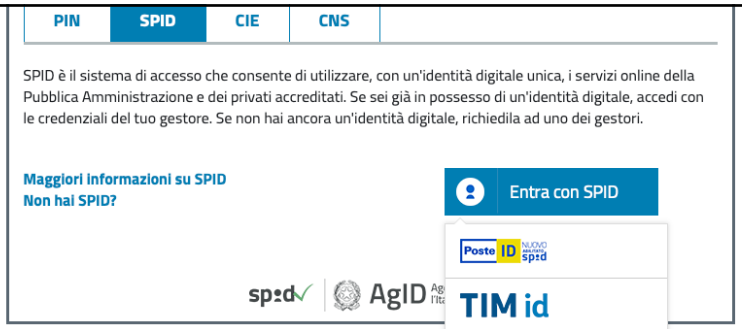
8. L'utente viene autenticato

Dott. ssa Angela Peduto- anpeduto@unisa.it
Dott. ssa Angela Peduto - anpeduto@unisa.it

83

Dott. ssa Angela Peduto- anpeduto@unisa.it

84



85

86

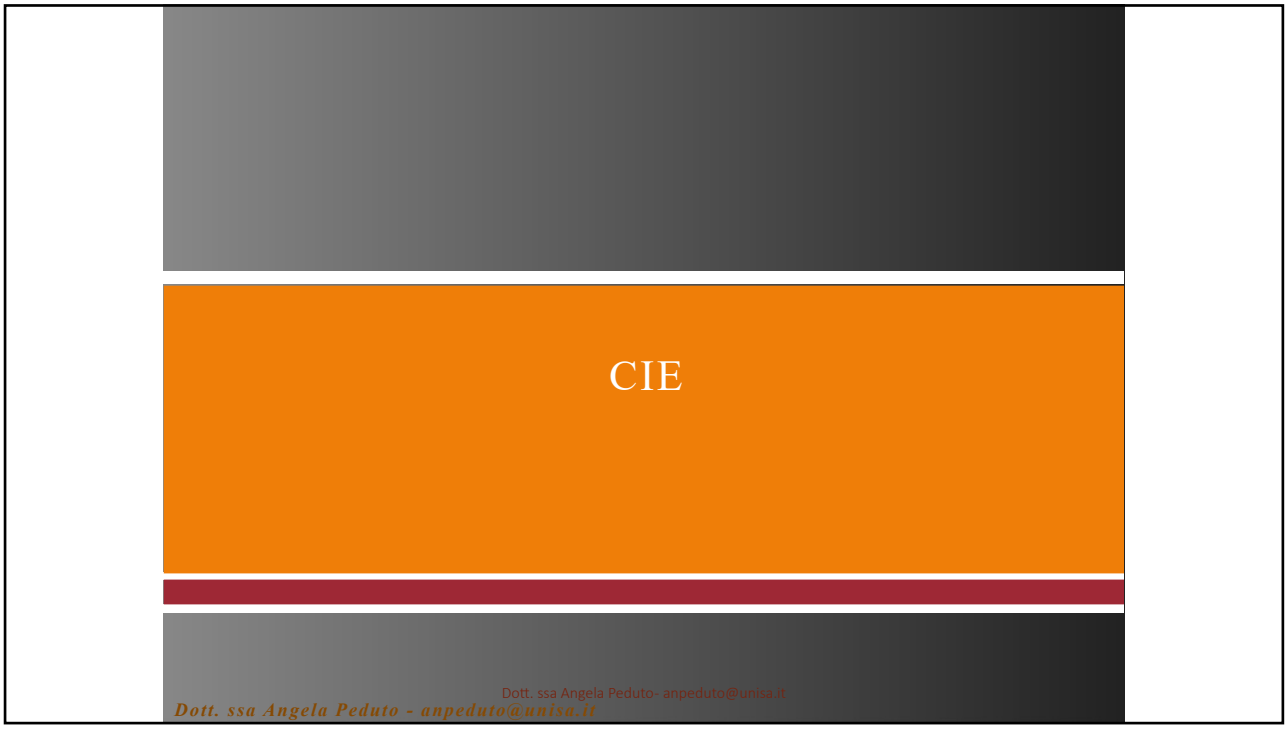

aruba.it ID
UTILIZZA
spid 2
IN ALTERNATIVA USA
spid 3
INPS - ISTITUTO NAZIONALE PREVIDENZA SOCIALE
Per accedere al servizio è richiesta l'immissione del codice temporaneo (OTP) generato dalla Sua credenziale.
Codice
Mostra OTP
Entra con SPID
Annulla
Tempo rimanente: 04m 52s
Tentativi rimanenti: 5
Dott. ssa Angela Peduto - anpeduto@unisa.it


One-Time Password
One-Time Password
368448
Generate

87


Gmail • angel.peduto@gmail.com • 2 min fa
Aruba ID
ArubaID - Notifica autenticazione
Gentile utente PedAng70,
la tua Identità Digitale è stata utilizzata per l'autenticazione a INPS - Istituto Nazionale Previdenza Sociale (http://www.inps.it) il 11/06/2020 alle 15:43:42 CEST.
L'operazione proviene dall'IP 93.40.230.85 e il livello richiesto dal fornitore di servizi è SPID2.
Se lo desideri puoi disattivare le notifiche di autenticazione effettuando l'accesso al pannello Self Care, sezione "Gestione Credenziali",
ARCHIVIA
RISPONDI

88



92

CIE

- La **Carta di Identità Elettronica (CIE)** è la **chiave di accesso**, garantita dallo Stato e rilasciata dal Ministero dell'Interno, che permette al cittadino di **autenticarsi in tutta sicurezza ai servizi online di enti e pubbliche amministrazioni** che ne consentono l'utilizzo.
- on la realizzazione del nodo eIDAS italiano si completa il progetto di **cittadinanza digitale europea**, che permette ai **titolari di una CIE** di accedere anche ai **servizi online di altri Paesi dell'Unione Europea**(ad esempio servizi universitari, bancari o delle pubbliche amministrazioni).

94

Carta Identità Elettronica CIE

- Documento con fotografia del titolare, rilasciato dai comuni. Contiene i dati anagrafici sull'involucro esterno, oleogrammi dell'Istituto Poligrafico dello Stato.

(l'allegato al Decreto 23 dicembre 2015 Ministero Interno descrive la struttura della nuova CIE)

- Permette di identificare il titolare anche senza l'ausilio del computer
- E' associata a codici PIN e PUK per l'identificazione informatica del cittadino

95

Autenticazione tramite CIE

possibili modalità di autenticazione:

- **modalità desktop**: si può accedere attraverso un **computer** collegato a un **lettore di smart card contactless** abilitato alla lettura della CIE, su cui bisogna avere installato il "Software CIE";
- **modalità mobile**: si può accedere con uno **smartphone dotato di interfaccia NFC** per la lettura della CIE, con l'app "CieID" installata;
- **modalità desktop con mobile**: l'accesso al servizio avviene da **computer**, utilizzando uno **smartphone dotato di interfaccia NFC** per la lettura della CIE, e l'app "CieID".

96

Sistema di recapito elettronico certificato PEC

Dott. ssa Angela Peduto- anpeduto@unisa.it

97

Servizio elettronico di recapito certificato

- Dal regolamento eIDAS «**servizio elettronico di recapito certificato**», un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove ***dell'avvenuto invio*** e ***dell'avvenuta ricezione dei dati***, e ***protegge i dati*** trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate;

Dott. ssa Angela Peduto- anpeduto@unisa.it

99

Servizio elettronico di recapito certificato

Tra questi requisiti:
- essere fornito da un prestatore di servizi qualificato;
- garantisce con un elevato grado di sicurezza l'identificazione del mittente
- garantisce l'identificazione del destinatario prima della trasmissione del messaggio
- l'invio e la ricezione sono garantiti da una firma elettronica avanzata (sigillo) in modo da escludere la possibilità di modifiche non rilevabili
- la data e l'ora di invio sono indicate da una validazione temporale elettronica qualificata

100

Posta Elettronica Certificata

eIDAS
- Servizio elettronico di recapito certificato

ITALIA
- PEC Posta Elettronica Certificata

101

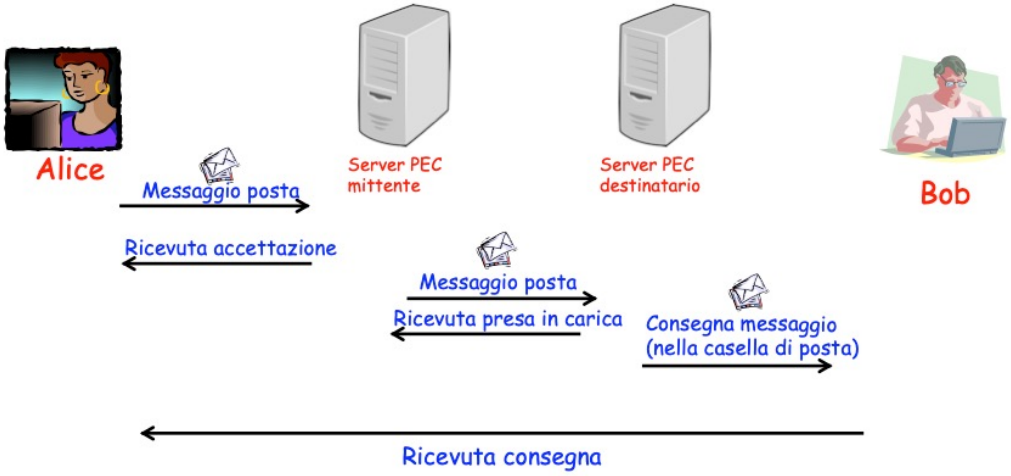
Gestori PEC

- A differenza della mail tradizionale la PEC fornisce certezze giuridiche equivalenti a quelle delle raccomandate con ricevuta di ritorno

- I servizi PEC non possono essere erogati da tutti gli ISP (internet service provider)
- I fornitori di servizi PEC devono possedere i requisiti specificati nell'art.14 del d.P.R. 11 febbraio 2005,n, 68

102

Ricevute PEC



103

RdAC e Orario di consegna / invio

La ricevuta di avvenuta consegna attesta che un messaggio è stato consegnato nella casella di posta elettronica del destinatario, ma non che questi l'abbia scaricato e letto

Il CAD riconosce alla PEC (o ad altri servizi di recapito certificato) il valore di notifica per posta e considera opponibili a terzi la data e l'ora presente nelle ricevute di accettazione e consegna

104

PEC – Funzionamento

- I canali di comunicazione dei messaggi sono realizzati con protocolli sicuri che garantiscono la riservatezza delle informazioni
- La ricevuta di accettazione è **firmata digitalmente** dal gestore del dominio del mittente ed ha valore giuridico spedizione (avvenuta)
- La busta di trasporto contiene:
  - Messaggio originale
  - Dati di certificazione
  - Firma digitale del gestore del mittente

106

Protocollazione dei messaggi PEC

Confermato **l'obbligo della registrazione di protocollo per:**

- le comunicazioni che pervengono o sono inviate attraverso la casella di PEC istituzionale e gli altri eventuali indirizzi di posta elettronica dichiarati all'Indice degli indirizzi delle amministrazioni pubbliche (www.indicepa.gov.it)
- i messaggi ricevuti o trasmessi attraverso l'indirizzo di PEC pubblicato sul sito istituzionale

I messaggi di PEC che rientrano nell'azione di una pubblica amministrazione devono

- essere **non solo protocollati, ma anche classificati, inseriti nei rispettivi fascicoli elettronici e conservati nell'archivio generale**

Dott. ssa Angela Peduto - anpeduto@unisa.it

107

Suggerimenti

In primo luogo, devono evitare l'eccessiva proliferazione degli indirizzi di PEC dichiarati all'Indice degli indirizzi delle amministrazioni pubbliche (www.indicepa.gov.it) e/o pubblicati sul loro sito istituzionale.

In secondo luogo, le pubbliche amministrazioni devono connettere direttamente le caselle di PEC istituzionali al sistema di gestione informatica dei documenti di cui al DPR n. 445/2000 (protocollo informatico).

Dott. ssa Angela Peduto - anpeduto@unisa.it

109

Firma digitale o pec? Quali differenze e similitudini

I due strumenti sono alquanto diversi tra loro anche se possono essere un ottima "accoppiata"

- la firma serve appunto per firmare un documento digitale;
- la pec serve per trasmettere in maniera sicura un informazione;

per entrambi il vero vantaggio è la piena validità legale.

113

Firma digitale o pec? Quali differenze e similitudini

Ad esempio se Paolo facesse un documento con sopra scritto "Io lavoro ai servizi segreti americani" che succede se lo firma digitalmente e lo invia per email?
E se invece non lo firma e lo invia per pec?
E se firma il documento e lo invia per pec?

114

Firma digitale o pec? Quali differenze e similitudini

Apparentemente uno potrebbe dire ma allora usiamo solo la PEC, ma non è così perché:

- la PEC è limitata nello spazio e nel tempo (può essere inviata ad un numero limitato di soggetti che comunque devono essere conosciuti e devono possedere la PEC come Paolo;
- la validità legale è limitata al testo scritto nel corpo e non nell'eventuale allegato che per avere piena validità deve essere firmato digitalmente;
- la trasmissione è riferito al momento X mentre un informazioni potrebbe essere lavorata molto tempo dopo;

115

Blockchain

116

Blockchain e Smart Contracts

- Sono una delle ultime novità dell'informatica
- Enorme interesse a partire dal 2014, salto di qualità nel 2017
- La Blockchain è vista come l'ultima rivoluzione ICT, con potenzialità pari a quelle di Internet nel '90
- Gli Smart Contracts promettono di rivoluzionare la finanza, il rapporto con le PA, l'Internet of Things, e molto altro...

117

Le basi matematiche e informatiche

- Le basi **matematiche** delle criptovalute sono:
  - la crittografia asimmetrica
  - le proprietà delle funzioni "hash"
- Le basi informatiche sono:
  - la rete Internet
  - l'architettura peer-to-peer
  - la capacità di calcolo intensivo

118

Crittografia asimmetrica

- Usata nella firma digitale
- Serve a garantire la proprietà esclusiva di un numero, la *chiave pubblica*, ovvero un *indirizzo* (*address*) da questa generato
- Tale numero è un'etichetta associata a un documento o a un bene (nel nostro caso è un importo di Bitcoin)
- L'utente genera due numeri molto grandi associati:
  - la chiave privata – per codificare un documento
  - la chiave pubblica, a partire da quella privata – per decodificarlo
  - … poi genera anche l'indirizzo (address) a partire dalla chiave pubblica

Impronte hash

- L'altra tecnologia chiave delle criptovalute è l'impronta hash.
- Una funzione hash H() associa un insieme qualsiasi di bit (ad es. un documento) a un numero di lunghezza data.
- Le caratteristiche delle funzioni hash sono:
  - H(x) è **molto diverso** da H(y), anche se x e y differiscono di **molto poco** (anche un solo bit).
  - Se **x è un documento**, è praticamente impossibile alterarlo in modo che il documento alterato abbia lo stesso valore hash dell'originale
  - Noto x, è facile calcolare H(x), ma noto H(x) si può risalire ad x solo per tentativi (provando tutte le combinazioni possibili).

Esempio di impronte hash

```
>echo ELLITTICO | sha256sum
```

0bafaefcd3d968bd632d02ef4e8d74e43a9052811cdc84dac76fde7cfff7ff07

```
>echo ELLITTICP | sha256sum
```

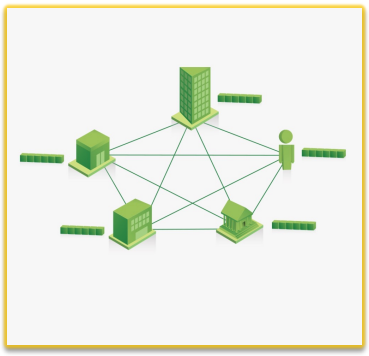
ba51d350f4bd38af2091f37f387dd17a892931d4ae45a5d7ddb8445b11f9e65a

- Le due stringhe “ELLITTICO” ed “ELLITTICP” differiscono di un solo bit, ma i rispettivi hash sono totalmente diversi
- L'algoritmo usato è SHA-2 (Secure Hash Algorithm 2) a 256 bit, standard NIST (National Institute of Standards and Technology)

121

Terminologia Blockchain

- è DLT (*Distributed Ledger Technology*) - sistema di contabilità condivisa rudimentale evoluzione del concetto Ledger (Libro Mastro)
- Tecnologicamente, è:
  - Database distribuito - registro pubblico (è possibile inserire e selezionare dati, ma non aggiornarli o eliminarli).
  - Computer distribuito: esegue contratti digitali
  - Basato su tecnologia **p2p** (peer-to-peer), crittografia e API



122

Conclusioni

Abbiamo visto strumenti diversi che possono essere usati in combinazione per supportare, ad esempio, lo smart working, queste soluzioni ci hanno permesso in questo particolare periodo, di continuare a lavorare, anche in remoto.

La tecnologia ha sicuramente un ruolo cardine nelle dinamiche del lavoro da casa, però, non è il solo elemento da tenere in considerazione poiché c'è la necessita di un adattamento nella gestione di spazi e tempi e dell'adozione di soluzioni efficaci, agili e veloci.

Dott. ssa Angela Peduto- anpeduto@unisa.it

123