Diritto dell'Informatica

Modulo Tecnico

A.A. 2020-2021

Melchiorre Monaca
melchiorre.monaca@unirc.it

1

Reti di Telecomunicazione

- Le reti di telecomunicazione
- Internet
- Il web
- Applicazioni

2

Vecchi mondi che non esistono più

Applicazioni isolate

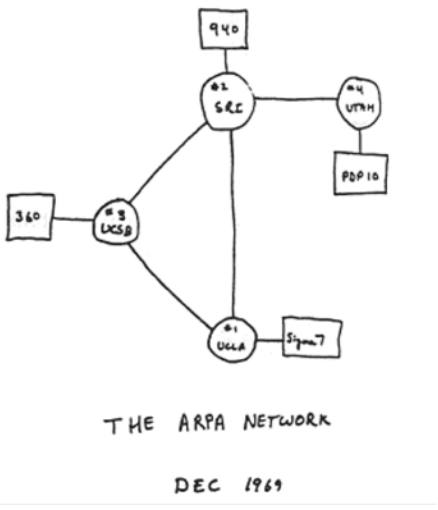
- Elaborazioni isolate
- Scambio dati su rete

Reti di telecomunicazione

- Reti dedicate ai servizi
- Nessuna elaborazione

3

Brevissima storia di Internet

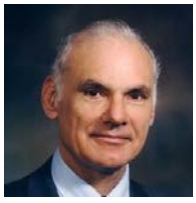


4

Storia di Internet: anni ‘60

- **1961:** Kleinrock – dimostra l’efficacia della commutazione di pacchetto grazie alla teoria delle code

- **1967:** Lawrence Roberts progetta ARPAnet (Advanced Research Projects Agency)

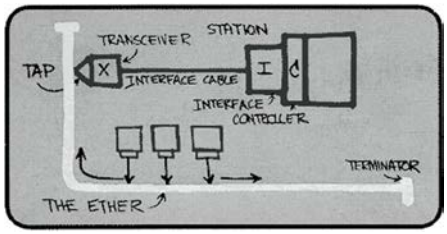


- **1969:** primo nodo di IMP (Interface Message Processor) di ARPAnet a UCLA

5

Storia di Internet: anni ‘70

- **1972:**
  - Nasce NCP (Network Control Protocol) il primo protocollo di Internet
  - Primo programma per la posta elettronica
  - ARPAnet ha 15 nodi
- **1970:**
  - ALOHAnet rete radio a pacchetti al Univ. of Hawaii
- **1974:**
  - Cerf and Kahn – definiscono i principi dell’internetworking (rete di reti)
- **1976:**
  - Nasce Ethernet nei laboratori di Xerox
- **1979:**
  - ARPAnet ha 200 nodi

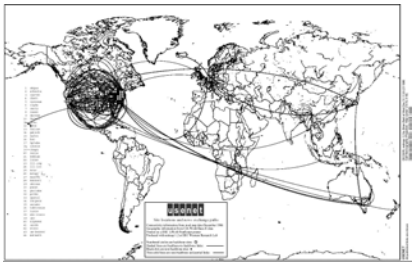


6

Storia di Internet: anni ‘80

- **1982:** definizione del protocollo SMTP per la posta elettronica
- **1983:** rilascio di TCP/IP che sostituisce NCP
- **1983:** definizione del DNS per la traduzione degli indirizzi IP
- **1985:** definizione del protocollo FTP
- **1988:** controllo della congestione TCP

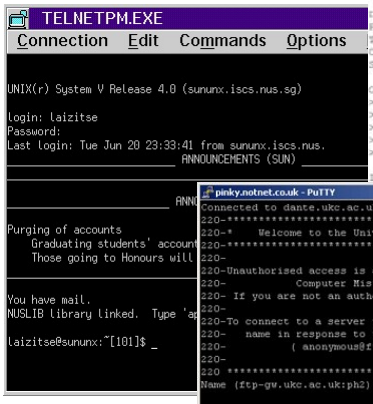
- **Nuove reti nazionali: Csnet, BITnet, NSFnet, Minitel**
- **100.000 host collegati**



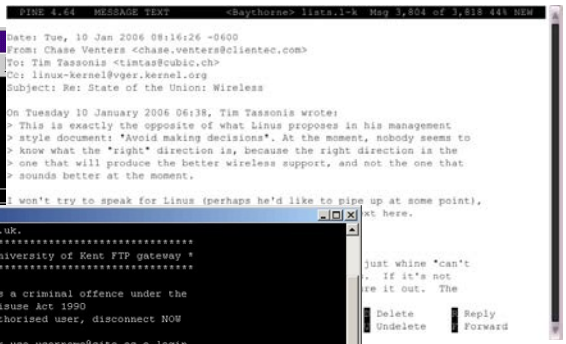
7

Storia di Internet: Le prime applicazioni

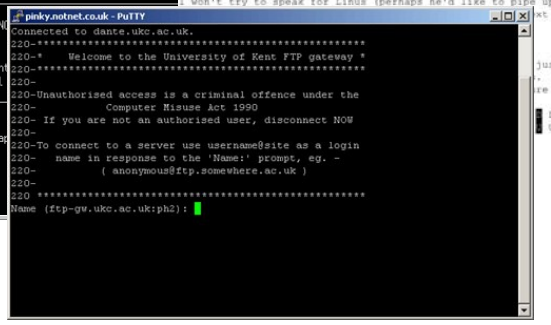
Telnet



Email



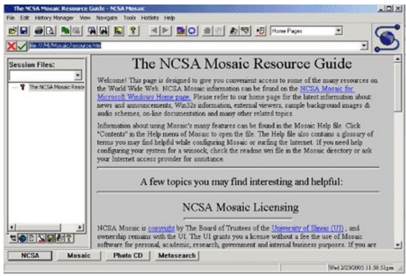
FTP



8

Storia di Internet: anni '90

- **1990:** ARPAnet viene dismessa
- **1991:** NSF lascia decadere le restrizioni sull'uso commerciale di NSFnet
- **Primi anni '90:** Tim Berners-Lee inventa il web al Cern di Ginevra
- **1994:** Mosaic, poi Netscape
- **Fine '90 :** commercializzazione del Web



9

Storia di Internet: anni '00

2000 – 2009:

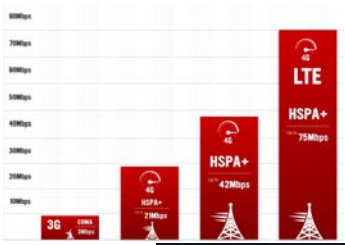
- Arrivano le "killer applications": messaggistica istantanea, condivisione di file P2P, IP Telephony, social networks
- La sicurezza di rete diventa un problema
- Centinaia di milioni di host, un miliardo di utenti
- Velocità nelle dorsali dell'ordine dei Gbps

10

Storia di Internet: anni ‘10

2010 – oggi:

- Esplosione della *Mobile Internet*
- Arrivano gli smart-phone
- La telefonia si trasferisce definitivamente su Internet
- I contenuti video diventano il traffico predominante sulla rete

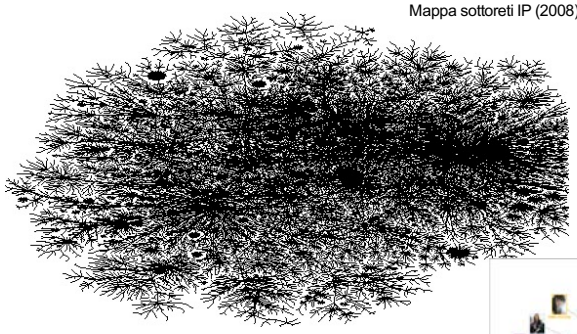


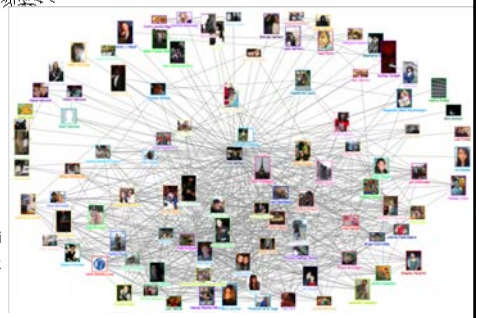
NETFLIX

11

Social netwoks

Mappa sottoreti IP (2008)





Esempio di topologia di social network

12

Sicurezza

KasperskyLab CyberThread Map - https://cybermap.kaspersky.com

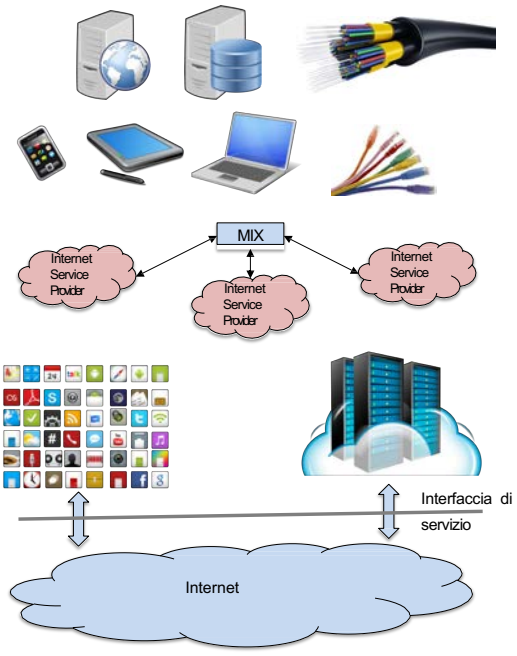
13

Cos'è Internet?

1) Una **infrastruttura fisica** fatta di componenti

2) Un'**architettura di rete**

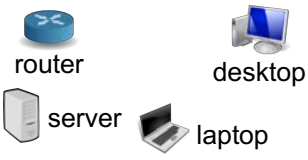
3) Un **servizio di comunicazione** usato dalle applicazioni e dai **protocolli di comunicazione** tra le componenti del sistema

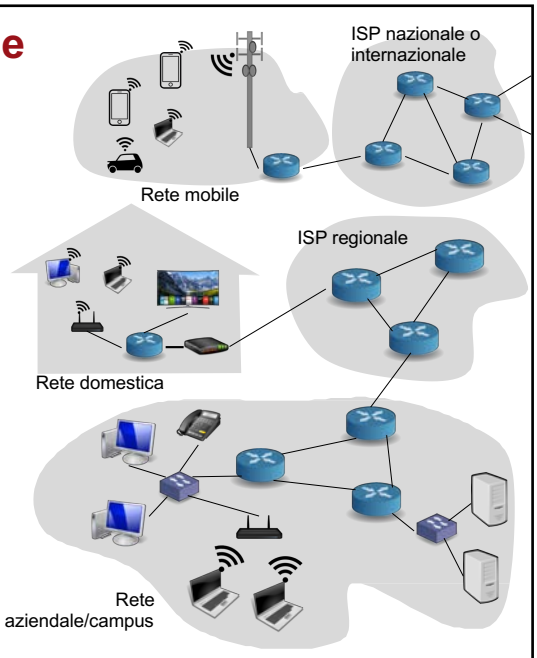


14

Componenti fisiche

- Milioni di computer connessi alla rete chiamati **host** = **terminali**
- Canali di comunicazione di diversi tipi (fibra, cavo, radio, satellite, …) **link** = **collegamenti**
- Nodi di rete chiamati **router** = **nodi**
- Altri nodi di rete locali (switch, access point, modem, …)

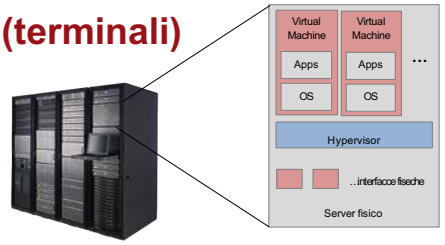




15

Componenti fisiche: host (terminali)

- Tutti gli **host** per la rete sono sistemi in grado di **inviare e ricevere informazioni** per le loro applicazioni finali
- Ma in realtà hanno caratteristiche molto diverse



Server fisici e virtuali per data center di servizi cloud

Dispositivi personali

Oggetti intelligenti

16

Componenti fisiche: link (collegamenti)

- I collegamenti possono essere di natura fisica molto diversa (fibra ottica, cavi coassiali, doppini, radio, ecc.)
- Differiscono anche per tecnologia di trasmissione dell'informazione
- E ovviamente per la velocità di trasmissione (rate) misurato in bit al secondo (b/s, Kb/s, Mb/s, Gb/s, Tb/s)


Fibra ottica


Cavi coassiali


Doppini


Antenne radio

17

Componenti fisiche: nodi di rete

- I nodi di rete di internet sono i **router** che operano su unità di informazione (sequenze di bit) finite dette pacchetti
- Esistono altri nodi di rete che a livello locale svolgono altre funzioni di collegamento
- Vedremo che il "livello" a cui opera un nodo di rete è un aspetto importante della tecnologia

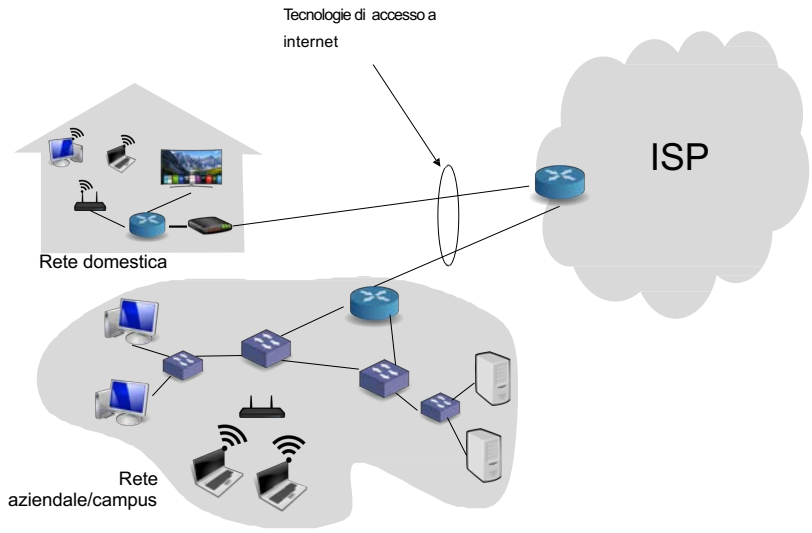

router


switch


access point

18

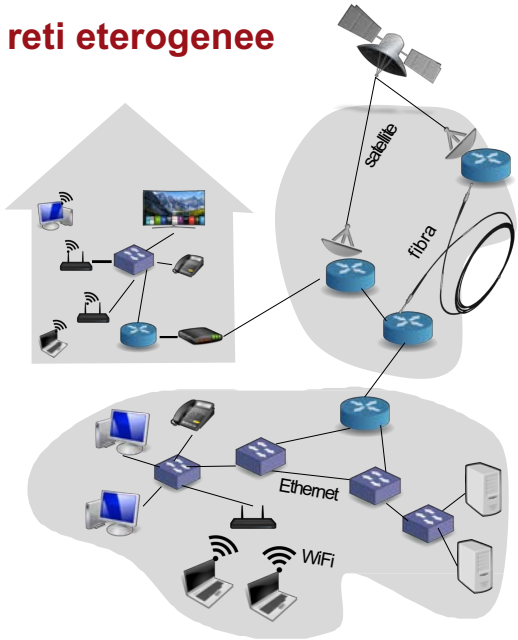
Architettura fisica: Accesso a Internet



19

Reti di reti: Insieme di reti eterogenee

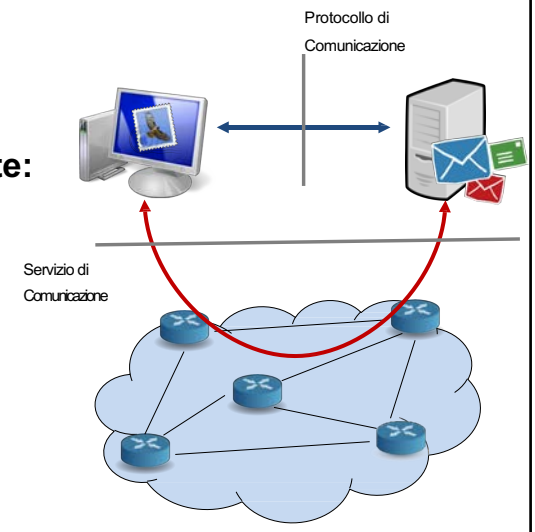
- Le diverse porzioni di rete sono composte da **tecnologie diverse**
- I router possono essere interconnessi da **link di vario tipo**
- Ma anche da "**sotto-reti**" che gestiscono internamente propri nodi e link
- Esempio: reti locali Ethernet e/o WiFi



20

Il servizio e i protocolli di comunicazione

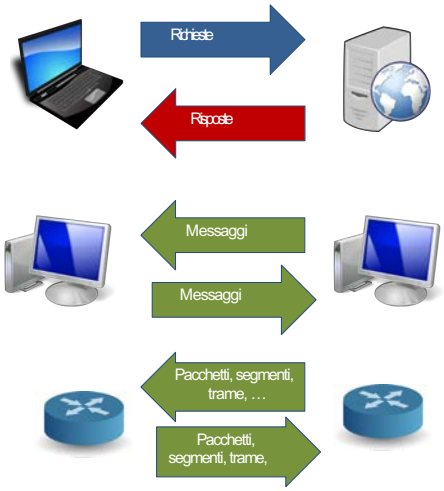
- **Infrastruttura di comunicazione consente le applicazioni distribuite:**
  - Web, email, games, e-commerce, file sharing
- **Protocolli di comunicazione per inviare e ricevere messaggi**



21

Protocolli di comunicazione: modelli

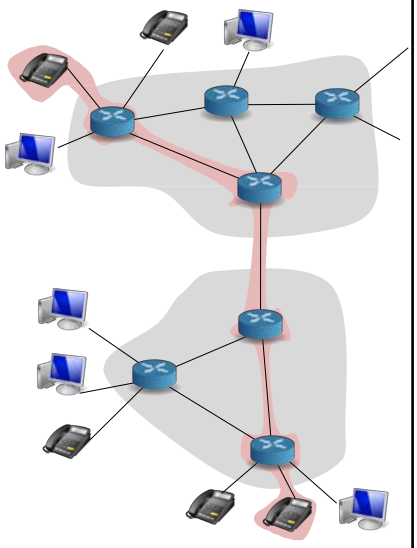
- **Modello client/server**
  - client chiedono il servizio, i server lo forniscono
  - I client fanno domande, i server rispondono
- **Modello peer-to-peer:**
  - Tutti i terminali collaborano senza distinzione di ruoli (o quasi)



22

Come funziona Internet?

- **Partiamo dal meccanismo di base**
- ***Come* può essere trasferita l'informazione in rete?**
  - Commutazione di circuito: circuito dedicato per chiamata
  - Commutazione di pacchetto: dati inviati in rete con messaggi

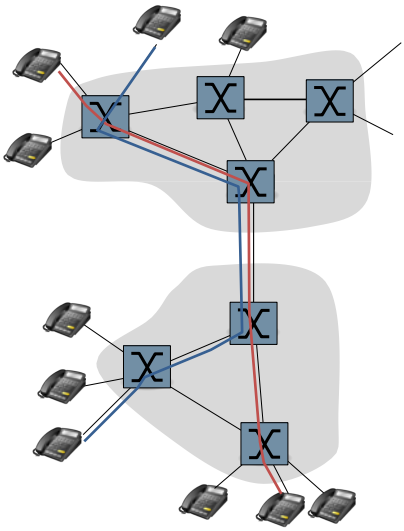


23

Commutazione di circuito

Le risorse per la comunicazione sono riservate per la chiamata

- **Esempio rete telefonica tradizionale**

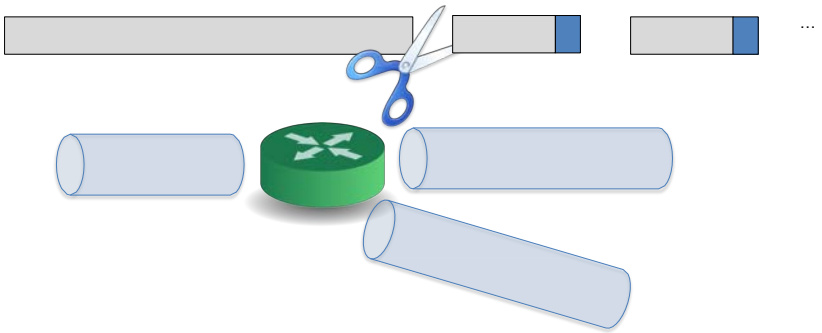


24

Commutazione di pacchetto

Il flusso di dati viene suddiviso in *pacchetti*

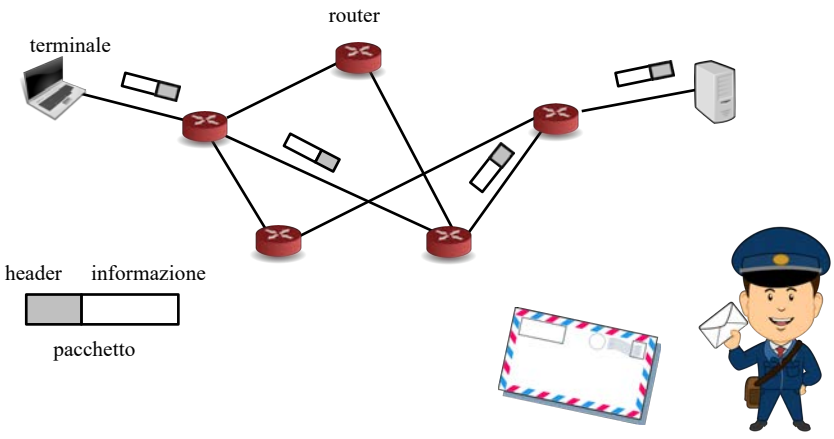
- I pacchetti di tutti gli utenti *condividono* le risorse di rete
- Ciascun pacchetto utilizza completamente il canale
- Le risorse vengono usate a seconda delle necessità



25

Commutazione di pacchetto

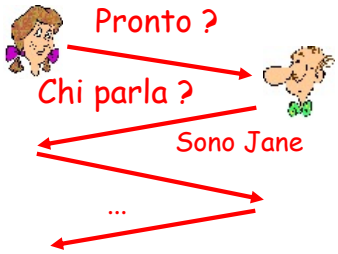
- **Informazione suddivisa in pezzi**
- **Collegamenti non suddivisi**



26

I problemi da risolvere

Facciamo una telefonata



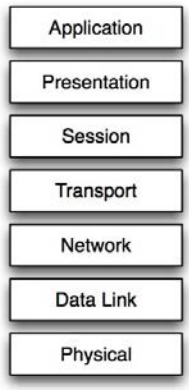
27

Scomponiamo il problema

- Collegamento fisico
- Indirizzamento
- Instradamento
- Trasporto dei dati
- Gestione della connessione
- Servizi

28

Il modello ISO/OSI



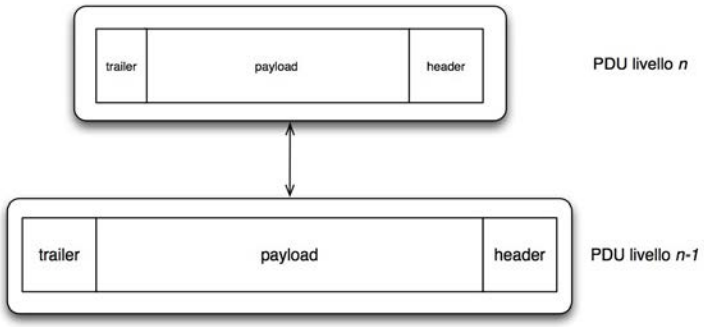
29

Incapsulamento

- Tante “buste”
- Header
- Payload
- Protocol Data Unit (PDU)
- Ogni livello gestisce l’header di sua competenza

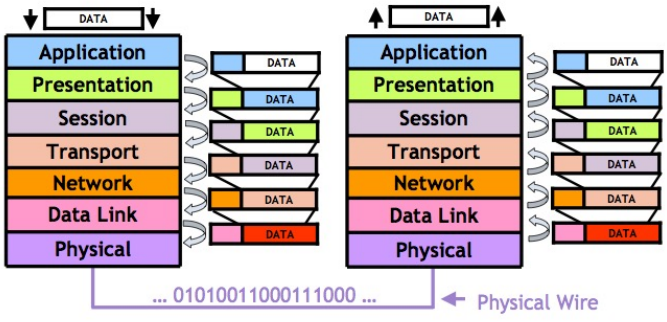
30

Incapsulamento



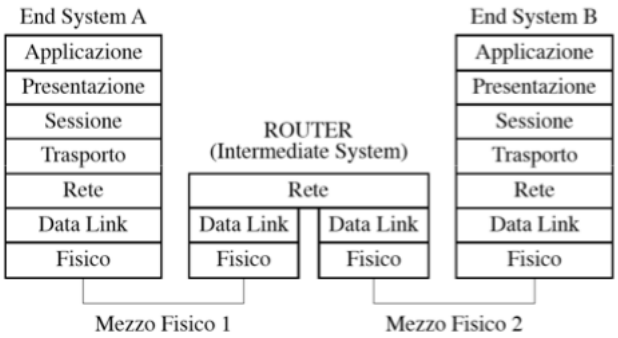
31

Il modello ISO/OSI



32

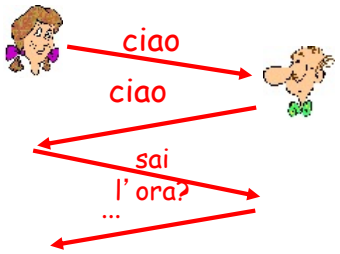
Il modello ISO/OSI



33

I Protocolli

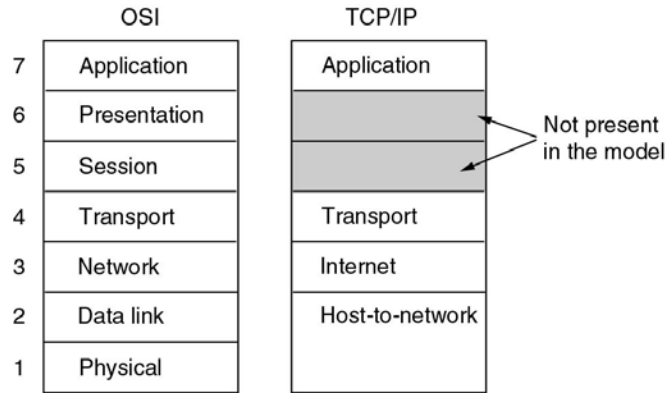
Conversazione



Connessione di rete

34

Il TCP/IP



35

Livello fisico: il mezzo trasmissivo

- Cavo elettrico
- Onde radio
- Fibra ottica
- Laser

36

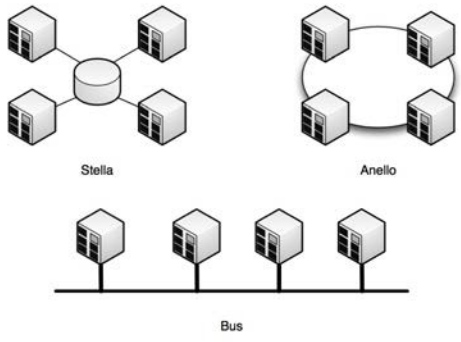
Classifichiamo

- PAN (Personal area network)
- LAN (Local area network)
- MAN (metropolitan area network)
- WAN (wide area network)

37

Livello fisico: topologia

- Point to Point
  - Stella
  - Anello
- Broadcast
  - Bus



38

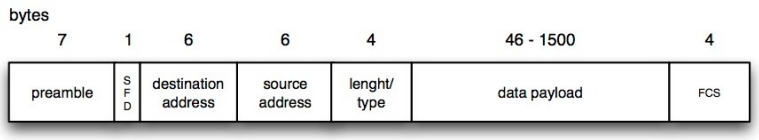
Livello Data Link

- Frammentazione
- Indirizzamento
- Controllo dell'errore
- Controllo di flusso

39

Livello Data Link: Ethernet

- Frame
- MAC ADDRESS



40

Livello Network

- Indirizzamento
- Routing
- Internetworking

41

Livello Network: IP

- Indirizzi IP
- Sottoreti
- Classi di Indirizzi
- Unicast, Broadcast, Multicast

42

Livello Network: IP

- Indirizzo host 1.2.3.4
  00000001.00000010.00000011.00000100
- Indirizzo network 1.2.3.0
  00000001.00000010.00000011.00000000
- Indirizzo broadcast 1.2.3.255
  00000001.00000010.00000011.11111111
- NetMask 255.255.255.0
  11111111. 11111111. 11111111. 00000000

43

Livello Network: IP

- Ind. host 1.2.3.4 AND netmask 255.255.255.0

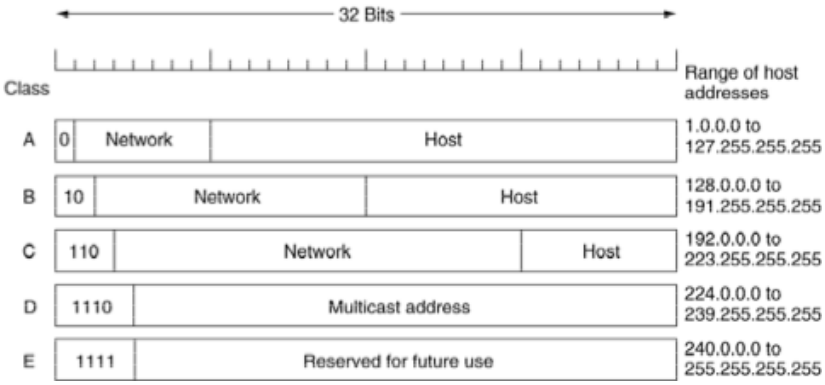
  00000001.00000010.00000011.00000100
  AND
  11111111.11111111.11111111.00000000

- Si ottiene indirizzo network 1.2.3.0

  00000001.00000010.00000011.00000000

44

Livello Network: IP - classi



45

Livello Network: IP – indirizzi privati

Class	First address	Last address	How many
A	10.0.0.0	10.255.255.255	16.777.216
B	172.16.0.0	172.31.255.255	1.048.576
C	192.168.0.0	192.168.255.255	65.536

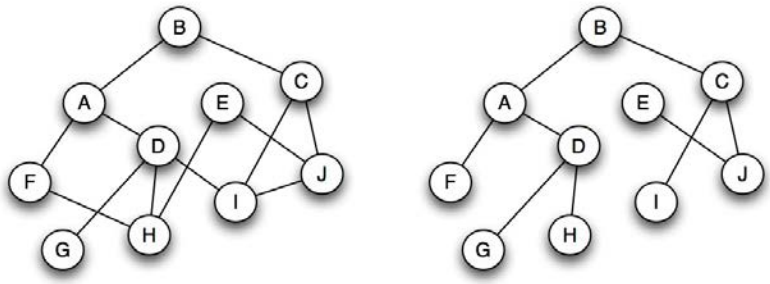
46

Livello Network: Routing

- Principio di ottimalità
- Routing statico
- Routing dinamico

47

Livello Network: Routing



48

Livello Network: Routing

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.167.111.254 to network 0.0.0.0

O    192.168.106.0/24 [110/2] via 192.167.111.12, 00:28:49, FastEthernet0/1
O    192.167.106.0/24 [110/2] via 192.167.111.12, 00:28:49, FastEthernet0/1
O    192.168.12.0/24 [110/11] via 192.167.111.254, 00:28:49, FastEthernet0/1
O    192.168.13.0/24 [110/11] via 192.167.111.254, 00:28:49, FastEthernet0/1
O    192.168.104.0/24 [110/2] via 192.167.111.16, 00:28:49, FastEthernet0/1
O    192.167.104.0/24 [110/2] via 192.167.111.16, 00:28:49, FastEthernet0/1
O    192.168.31.0/24 [110/28] via 192.167.111.254, 00:28:49, FastEthernet0/1
O    192.168.105.0/24 [110/2] via 192.167.111.16, 00:28:49, FastEthernet0/1
O    192.167.105.0/24 [110/2] via 192.167.111.16, 00:28:49, FastEthernet0/1
O    192.168.8.0/24 [110/25] via 192.167.111.254, 00:28:49, FastEthernet0/1
O    192.168.110.0/24 [110/2] via 192.167.111.16, 00:28:49, FastEthernet0/1
O    192.167.110.0/24 [110/2] via 192.167.111.96, 00:28:49, FastEthernet0/1
     192.168.111.0/30 is subnetted, 6 subnets
C       192.168.111.4 is directly connected, Serial0/0.1
O       192.168.111.0 [110/24] via 192.167.111.254, 00:28:49, FastEthernet0/1
O       192.168.111.12 [110/24] via 192.167.111.254, 00:28:49, FastEthernet0/1
O       192.168.111.8 [110/24] via 192.167.111.254, 00:28:49, FastEthernet0/1
O       192.168.111.16 [110/24] via 192.167.111.254, 00:28:49, FastEthernet0/1
O       192.168.111.96 [110/24] via 192.167.111.254, 00:28:49, FastEthernet0/1
C    192.167.111.0/24 is directly connected, FastEthernet0/1
O    192.167.108.0/24 [110/2] via 192.167.111.20, 00:28:58, FastEthernet0/1
C    192.168.109.0/24 is directly connected, FastEthernet0/0
C    192.167.109.0/24 is directly connected, FastEthernet0/0
......
```

49

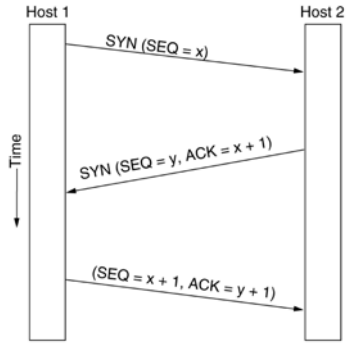
Livello Transport

- Controllo della connessione
  - Connection less (UDP)
  - Connection oriented (TCP)
- Controllo di flusso
- Riordino dei TPDU

50

Livello Transport: TCP

- Three-way handshake



51

Livello Transport: TCP

- Socket

Port	Protocol	Use
21	FTP	File transfer
23	Telnet	Remote login
25	SMTP	E-mail
69	TFTP	Trivial File Transfer Protocol
79	Finger	Lookup info about a user
80	HTTP	World Wide Web
110	POP-3	Remote e-mail access
119	NNTP	USENET news

52

Applicazioni

- Dns
- Web
- E-MAIL
- Motori di ricerca
- Content delivery
- Peer to Peer
- Ip Telephony e Videoconferenza
- Chat
- Streaming

53

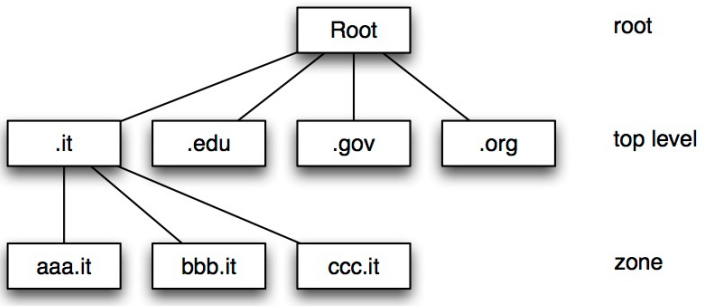
DNS – The Domain Name System

- The DNS Name Space
- Resource Records
- Name Servers

54

The DNS Name Space

A sample of the Internet domain name space.



55

Resource Records

The principal DNS resource records types.

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

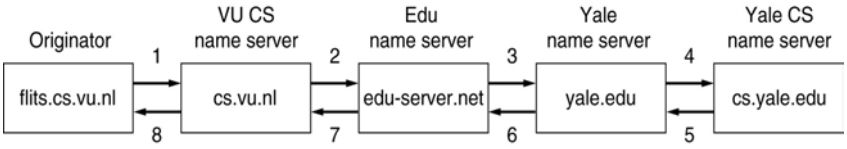
56

Resource Records (2)

```
; Authoritative data for cs.vu.nl
cs.vu.nl.        86400  IN  SOA     star boss (952771,7200,7200,2419200,86400)
cs.vu.nl.        86400  IN  TXT     "Divisie Wiskunde en Informatica."
cs.vu.nl.        86400  IN  TXT     "Vrije Universiteit Amsterdam."
cs.vu.nl.        86400  IN  MX      1 zephyr.cs.vu.nl.
cs.vu.nl.        86400  IN  MX      2 top.cs.vu.nl.

flits.cs.vu.nl.  86400  IN  HINFO   Sun Unix
flits.cs.vu.nl.  86400  IN  A       130.37.16.112
flits.cs.vu.nl.  86400  IN  A       192.31.231.165
flits.cs.vu.nl.  86400  IN  MX      1 flits.cs.vu.nl.
flits.cs.vu.nl.  86400  IN  MX      2 zephyr.cs.vu.nl.
flits.cs.vu.nl.  86400  IN  MX      3 top.cs.vu.nl.
www.cs.vu.nl.    86400  IN  CNAME   star.cs.vu.nl
ftp.cs.vu.nl.    86400  IN  CNAME   zephyr.cs.vu.nl

rowboat                 IN  A       130.37.56.201
                        IN  MX      1 rowboat
                        IN  MX      2 zephyr
                        IN  HINFO   Sun Unix

little-sister           IN  A       130.37.62.23
                        IN  HINFO   Mac MacOS

laserjet                IN  A       192.31.231.216
                        IN  HINFO   "HP Laserjet IIISi" Proprietary
```

57

Name Servers (2)



How a resolver looks up a remote name in eight steps.

58

Electronic Mail

- Architecture and Services
- The User Agent
- Message Formats
- Message Transfer
- Final Delivery

59

Electronic Mail (2)

Some smileys. They will not be on the final exam :-).

Smiley	Meaning	Smiley	Meaning	Smiley	Meaning
:-)	I'm happy	=|:-)	Abe Lincoln	:+)	Big nose
:-(	I'm sad/angry	=):-)	Uncle Sam	:-))	Double chin
:-|	I'm apathetic	*<:-)	Santa Claus	:-{)	Mustache
;-)	I'm winking	<:-(	Dunce	#:-)	Matted hair
:-(O)	I'm yelling	(-:	Australian	8-)	Wears glasses
:-(*)	I'm vomiting	:-)X	Man with bowtie	C:-)	Large brain

60

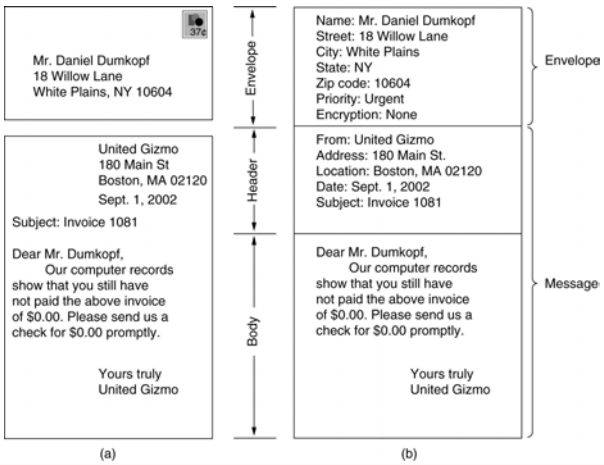
E-Mail Architecture and Services

Basic functions

- Composition
- Transfer
- Reporting
- Displaying
- Disposition

61

The User Agent



62

Reading E-mail

63

Reading E-mail

```
Return-Path: it_it_ndt_bounces@insideapple.apple.com
Received: from mta.unime.it (LHLO mta.unime.it) (192.167.101.20) by
 mail1.unime.it with LMTP; Wed, 14 Mar 2012 08:52:02 +0100 (CET)
Received: from localhost (localhost [127.0.0.1])
     by mta.unime.it (Postfix) with ESMTP id 3D6E6120DA912
     for <monaca@unime.it>; Wed, 14 Mar 2012 08:52:02 +0100 (CET)
X-Spam-Flag: NO
X-Spam-Score: -1.313
X-Spam-Level:
X-Spam-Status: No, score=-1.313 tagged_above=-10 required=10 tests=[AWL=0.689,
     BAYES_00=-2.599, HTML_IMAGE_RATIO_06=0.001, HTML_MESSAGE=0.001,
     SPF_HELO_PASS=-0.001, SPF_SOFTFAIL=0.596]
Received: from mta.unime.it ([127.0.0.1])
     by localhost (mta.unime.it [127.0.0.1]) (amavisd-new, port 10024)
     with ESMTP id ibJHXOPT9FCg for <monaca@unime.it>;
     Wed, 14 Mar 2012 08:52:00 +0100 (CET)
Received: from smtp1.unime.it (smtp.unime.it [192.167.101.11])
     by mta.unime.it (Postfix) with ESMTP id 6FB7712090C1A
     for <melchiorre.monaca@unime.it>; Wed, 14 Mar 2012 08:52:00 +0100 (CET)
Received: from smtp1.unime.it (localhost.localdomain [127.0.0.1])
     by localhost (Email Security Appliance) with SMTP id 5AD98101E47C_F604E20B
     for <melchiorre.monaca@unime.it>; Wed, 14 Mar 2012 07:52:00 +0000 (GMT)
Received: from msbadger0102.apple.com (msbadger0102.apple.com [17.254.6.109])
     by smtp1.unime.it (Sophos Email Appliance) with ESMTP id 2EAAD1018AB5_F604E1EF
     for <melchiorre.monaca@unime.it>; Wed, 14 Mar 2012 07:51:57 +0000 (GMT)
DKIM-Signature: v=1; a=rsa-sha1; d=new.itunes.com; s=itunes; c=relaxed/simple;
     q=dns/txt; i=@new.itunes.com; t=1331711517;
     h=From:Subject:Date:To:MIME-Version:Content-Type;
     bh=cdEntTCoIDlRPDGUy0el70w60k4=;
     b=RMIKXvkLn1BFm6uyqeBbInpD3XJmQL8TxGPMlDQj9nrEb5kPKFEHK//DtNcd0fnX
     mH7VOcnDyRFFIEmpZEyN4g==;
Date: Wed, 14 Mar 2012 00:51:57 -0700
From: iTunes <itunes_it@new.itunes.com>
To: melchiorre.monaca@unime.it
```

64

Message Formats – RFC 822

RFC 822 header fields

Header	Meaning
To:	E-mail address(es) of primary recipient(s)
Cc:	E-mail address(es) of secondary recipient(s)
Bcc:	E-mail address(es) for blind carbon copies
From:	Person or people who created the message
Sender:	E-mail address of the actual sender
Received:	Line added by each transfer agent along the route
Return-Path:	Can be used to identify a path back to the sender

65

Message Formats – RFC 822 (2)

Header	Meaning
Date:	The date and time the message was sent
Reply-To:	E-mail address to which replies should be sent
Message-Id:	Unique number for referencing this message later
In-Reply-To:	Message-Id of the message to which this is a reply
References:	Other relevant Message-Ids
Keywords:	User-chosen keywords
Subject:	Short summary of the message for the one-line display

66

MIME – Multipurpose Internet Mail Extensions

Problems with international languages:

- Languages with accents (French, German).
- Languages in non-Latin alphabets (Hebrew, Russian).
- Languages without alphabets (Chinese, Japanese).
- Messages not containing text at all (audio or images).

67

MIME (2)

RFC 822 headers added by MIME.

Header	Meaning
MIME-Version:	Identifies the MIME version
Content-Description:	Human-readable string telling what is in the message
Content-Id:	Unique identifier
Content-Transfer-Encoding:	How the body is wrapped for transmission
Content-Type:	Type and format of the content

68

MIME (3)

Type	Subtype	Description
Text	Plain	Unformatted text
	Enriched	Text including simple formatting commands
Image	Gif	Still picture in GIF format
	Jpeg	Still picture in JPEG format
Audio	Basic	Audible sound
Video	Mpeg	Movie in MPEG format
Application	Octet-stream	An uninterpreted byte sequence
	Postscript	A printable document in PostScript
Message	Rfc822	A MIME RFC 822 message
	Partial	Message has been split for transmission
	External-body	Message itself must be fetched over the net
Multipart	Mixed	Independent parts in the specified order
	Alternative	Same message in different formats
	Parallel	Parts must be viewed simultaneously
	Digest	Each part is a complete RFC 822 message

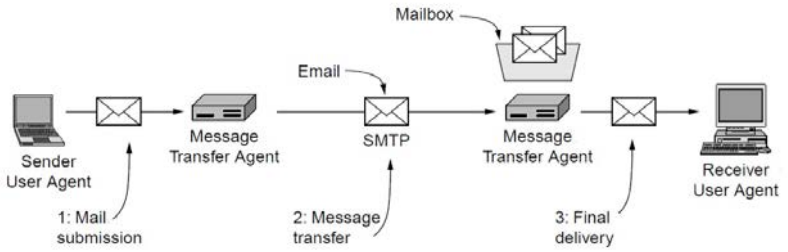
69

MIME (4)

```
From: elinor@abcd.com
To: carolyn@xyz.com
MIME-Version: 1.0
Message-Id: <0704760941.AA00747@abcd.com>
Content-Type: multipart/alternative; boundary=qwertyuiopasdfghjklzxcvbnm
Subject: Earth orbits sun integral number of times

This is the preamble. The user agent ignores it. Have a nice day.

--qwertyuiopasdfghjklzxcvbnm
Content-Type: text/enriched

Happy birthday to you
Happy birthday to you
Happy birthday dear <bold> Carolyn </bold>
Happy birthday to you

--qwertyuiopasdfghjklzxcvbnm
Content-Type: message/external-body;
        access-type="anon-ftp";
        site="bicycle.abcd.com";
        directory="pub";
        name="birthday.snd"

content-type: audio/basic
content-transfer-encoding: base64
--qwertyuiopasdfghjklzxcvbnm--
```

70

E-mail Delivery



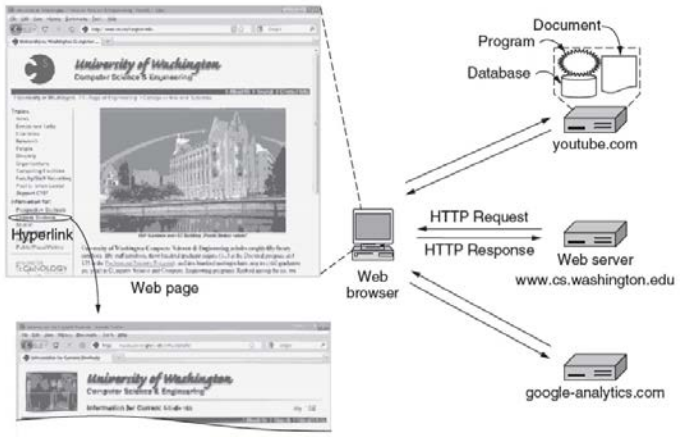
71

Fetch E-mail

- POP 3
- IMAP

72

The World Wide Web



73

URLs – Uniform Resource Locators

Some common URLs.

Name	Used for	Example
http	Hypertext (HTML)	http://www.cs.vu.nl/~ast/
ftp	FTP	ftp://ftp.cs.vu.nl/pub/minix/README
file	Local file	file:///usr/suzanne/prog.c
news	Newsgroup	news:comp.os.minix
news	News article	news:AA0134223112@cs.utah.edu
gopher	Gopher	gopher://gopher.tc.umn.edu/11/Libraries
mailto	Sending e-mail	mailto:JohnUser@acm.org
telnet	Remote login	telnet://www.w3.org:80

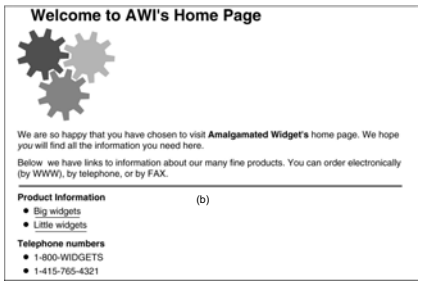
74

HTML

- HyperText Markup Language

```
<html>
<head><title> AMALGAMATED  WIDGET, INC. </title> </head>
<body> <h1> Welcome to AWI's Home Page</h1>
<img src="http://www.widget.com/images/logo.gif" ALT="AWI Logo"> <br>
We are so happy that you have chosen to visit <b> Amalgamated Widget's </b>
home page. We hope <i> you </i> will find all the information you need here.
<p>Below we have links to information about our many fine products.
You can order electronically (by WWW), by telephone, or by fax. </p>
<hr>
<h2> Product information </h2>
<ul>
   <li> <a href="http://widget.com/products/big"> Big widgets </a>
   <li> <a href="http://widget.com/products/little"> Little widgets </a>
</ul>
<h2> Telephone numbers</h2>
<ul>
   <li> By telephone: 1-800-WIDGETS
   <li> By fax: 1-415-765-4321
</ul>
</body>
</html>
```

(a)



(b)

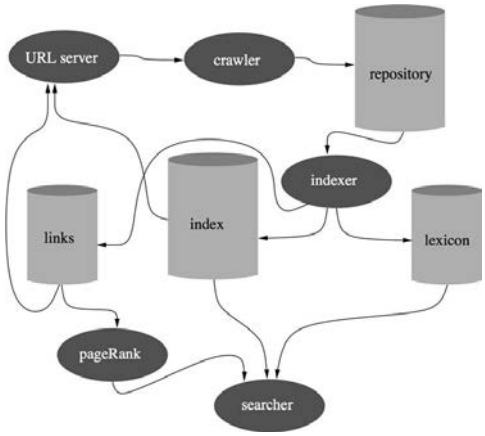
75

HTML (2)

Tag	Description
<html> ... </html>	Declares the Web page to be written in HTML
<head> ... </head>	Delimits the page's head
<title> ... </title>	Defines the title (not displayed on the page)
<body> ... </body>	Delimits the page's body
<h*n*> ... </h*n*>	Delimits a level *n* heading
...	Set ... in boldface
...	Set ... in italics
...	Center ... on the page horizontally
...	Brackets an unordered (bulleted) list
...	Brackets a numbered list
	Starts a list item (there is no)
 	Forces a line break here
<p>	Starts a paragraph
<hr>	Inserts a Horizontal rule
<img src="...">	Displays an image here
 ... 	Defines a hyperlink

76

Search Engines



77

SICUREZZA

78

Definizioni

- Con il termine "sicurezza" si intende l'insieme delle misure tese ad assicurare a ciascun utente autorizzato (e a nessun altro) tutti e soli i servizi previsti per quell'utente, nei tempi e nelle modalità previste. In generale, secondo la definizione ISO, *la sicurezza è l'insieme delle misure atte a garantire la disponibilità, la integrità e la riservatezza delle informazioni gestite*
- In un contesto di sistemi distribuiti, in cui la rete diventa un elemento fondamentale, si parla di *sicurezza di rete* ad indicare *l'insieme di procedure, pratiche e tecnologie per proteggere le risorse, gli utenti e le organizzazioni che operano in rete*. Un approccio sistematico alla sicurezza di rete prevede la considerazione di tre elementi fondamentali:
  - Evento Indesiderato (attacco). Ogni evento che compromette la sicurezza.
  - Meccanismo. Ogni soluzione progettata per scoprire, prevenire e recuperare un attacco.
  - Servizio. Ogni servizio che migliora la sicurezza del sistema e delle informazioni in transito. I servizi fronteggiano gli attacchi, e fanno uso di uno o più meccanismi per essere forniti.

79

Sicurezza

- **Integrità**
  - protezione da modifiche (o cancellazioni) non autorizzate dei dati trasmessi
  - garantire l'integrità di un messaggio significa assicurare che il messaggio ricevuto sia esattamente quello spedito dal mittente.
- **Autenticazione**
  - chi sei? Possibilità di identificare in modo certo e univoco chi invia e riceve i dati
  - può essere semplice (solo mittente) o mutua (sia mittente che destinatario)
- **Non ripudio**
  - prova formale, utilizzabile anche a termine di legge, per dimostrare che una certa persona ha sottoscritto (firmato) un documento
- **Integrità e autenticazione sono condizioni necessarie per garantire che mittente e destinatario non possano negare di aver inviato e ricevuto il documento firmato**

80

Sicurezza

- **Autorizzazione**
  - cosa puoi fare?
  - capacità di controllare le operazioni che un utente autenticato può effettuare e le risorse a cui può accedere
- **Riservatezza**
  - protezione da letture non autorizzate dei dati
  - ha lo scopo di impedire l'utilizzo illegittimo di informazioni riservate
- **Disponibilità**
  - capacità di garantire l'accesso all'infrastruttura e la fruizione dei servizi agli utenti autorizzati

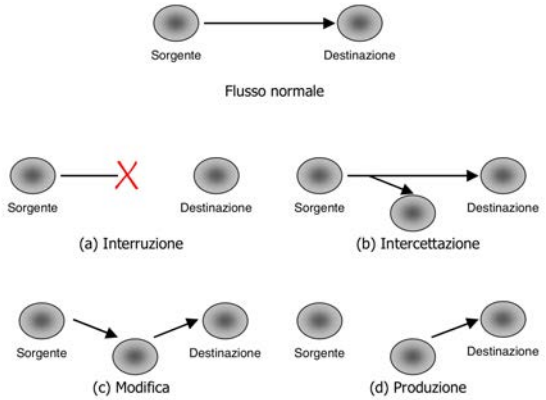
81

Attacchi alla sicurezza

- **Attacchi passivi**
  - Obiettivo: entrare in possesso di informazioni riservate
  - Compromettono la riservatezza e l'autenticazione
  - È più facile intervenire con la prevenzione che rilevarne la presenza
- **Attacchi attivi**
  - Obiettivo: alterare le informazioni e/o danneggiare le risorse
  - Compromettono l'integrità e la disponibilità
  - Molto spesso gli attacchi passivi sono effettuati per ottenere le informazioni necessarie a iniziare un attacco attivo

82

Categorie di attacchi



83

Interruzione

- Una parte del sistema viene distrutta o diventa non utilizzabile
- Attacco alla disponibilità del sistema

84

Intercettazione

- Un soggetto non autorizzato ottiene accesso ad una componente del sistema. Questo è un attacco alla riservatezza. Gli attacchi di intercettazione possono richiedere un attacco preventivo a livello fisico per installare dispositivi pirata o per agganciarsi alla rete, e di produzione per installare software di supporto alla intercettazione.
- Le tecniche comunemente utilizzate sono basate su:
  - analizzatori di traffico su rete (locale o geografica);
  - applicazioni di analisi del traffico su rete (**sniffing**);
  - server pirata che, attaccando alcuni router, si spacciano come server originali. Tale attacco consiste nel cambiare le tavole di instradamento di un router (**spoofing**);
  - programmi che emulano servizi del sistema registrando al contempo le informazioni riservate digitate dall'utente. Ad esempio viene emulato il programma di login, durante il quale l'utente digita username e password, in maniera da ottenere la password dell'utente (**password cracking**).
  - Gli attacchi di intercettazione possono sfruttare debolezze intrinseche di protocolli e software di rete, o poco accorte configurazioni del sistema operativo. Gli attacchi di intercettazione possono sfruttare il fatto che un utente abbia disatteso qualche norma comportamentale imposta dalla politica di sicurezza: infatti quando il sistema non prevede strumenti evoluti per il riconoscimento dell'utente (chiave hardware, lettore di impronte digitali, etc.), l'accesso al sistema tramite password illegale è uno degli attacchi di intrusione più frequenti

85

Modifica

- Un soggetto non autorizzato entra in possesso di una componente del sistema, la modifica e la introduce di nuovo nel sistema.
- Attacco all'integrità

86

Produzione

- Un soggetto non autorizzato produce componenti nuove e le immette nel sistema.
- Gli attacchi che fanno uso di queste tecniche non sono tesi ad accedere a servizi ed informazioni, ma semplicemente a degradare la operatività del sistema.
- Minacciano tipicamente la integrità e la disponibilità, più raramente (e indirettamente) la riservatezza.
- Esistono diverse tecniche
  - virus
  - worm
  - denial of service: si tratta di una famiglia di tecniche tese a fare in modo che il sistema neghi l'accesso a servizi ed informazioni anche ad utenti regolarmente autorizzati. Gli attacchi che usano queste tecniche minacciano quindi i requisiti di disponibilità del sistema. Tpiche tecniche denial of service consistono ad esempio nel paralizzare il traffico sulla rete generando falsi messaggi di errore o intasandola con traffico di disturbo generato appositamente

87

Mapping e port scanning

Obiettivo: determinare quali sono gli host attivi in una rete e quali sono i servizi offerti

- **Mapping**
  - ricostruzione di quali sono gli indirizzi IP attivi di una stessa rete
  - Es. Uso del ping o di altre utility per l'esplorazione di una rete
- **Port scanning**
  - Contatto sequenziale dei numeri di porta di uno stesso host per vedere cosa succede
  - I numeri di porta sono contattati sia con segmenti TCP (es. con telnet) che con segmenti UDP
  - Es. Uso di telnet o di di altre utility per la scansione delle porte

88

Sniffing

- **Lettura dei pacchetti destinati ad un altro nodo della rete**
  - Quando i dati viaggiano su una rete a mezzo condiviso (come sono tipicamente le LAN) è possibile da un qualsiasi punto della rete intercettare i pacchetti in transito destinati ad altri host
- **L'intercettazione dei dati è fatta attraverso appositi programmi, detti sniffer, che:**
  - mettono la scheda di rete Ethernet in modalità promiscua
  - convertono i dati raccolti in una forma leggibile ricostruendo i pacchetti dei protocolli di livello più alto
  - filtrano i pacchetti in base a criteri definibili dall'utente

89

Packet sniffing

- lettura dei pacchetti destinati ad un altro nodo della rete
- facile da fare in reti broadcast (es. LAN) o nei nodi di smistamento
- attacchi:
  - permette di intercettare qualunque cosa (password, dati, ...)
- contromisure:
  - reti non broadcast
  - crittografia dei pacchetti

90

User account spoofing

- **L'identità elettronica degli utenti può essere sostituita intercettando le credenziali di autenticazione**
  - sia al di fuori del sistema (social enginering)
  - sia sfruttando vulnerabilità dei sistemi interni (malware)
  - sia mentre queste credenziali transitano sulla rete
- **I problemi più gravi si hanno**
  - quando l'abuso produce gravi violazioni alle norme vigenti
  - quando l'abuso avviene in un contesto commerciale e dà origine a obblighi per la persona la cui identità è stata utilizzata impropriamente
  - quando viene carpita l'identità dell'amministratore del sistema
- **Sono colpiti: l'autenticazione, l'integrità, il non ripudio e la riservatezza**

91

Address spoofing

- **IP spoofing**
  - Falsificazione dell'indirizzo di rete del mittente
  - Il sistema che effettua l'attacco si spaccia per un diverso IP
  - Il sistema che subisce l'attacco invia le risposte all'host effettivamente corrispondente all'IP utilizzato per lo spoofing
- **DNS spoofing**
  - Falsificazione del nome simbolico
  - La richiesta di una pagina web o di un altro servizio è fatta al fornitore sbagliato
  - Basato sulla modifica del DNS server a cui la vittima si rivolge (direttamente o indirettamente)

92

Data spoofing

- **Alterazione dei dati nel corso di una comunicazione**
  - Si utilizza uno dei meccanismi di spoofing precedentemente descritti
  - Si prende il controllo di un canale di comunicazione e su questo si inseriscono, cancellano o modificano dei pacchetti

93

Denial-of-service (DoS)

- si tiene impegnato un host in modo che non possa fornire i suoi servizi
- esempi:
  - saturazione della posta / log
  - ping flooding (“guerra dei ping”)
  - SYN attack
- attacchi:
  - impedisce l’uso di un sistema / servizio
- contromisure:
  - nessuna definitiva
  - limitare ICMP
  - hardening dei sistemi

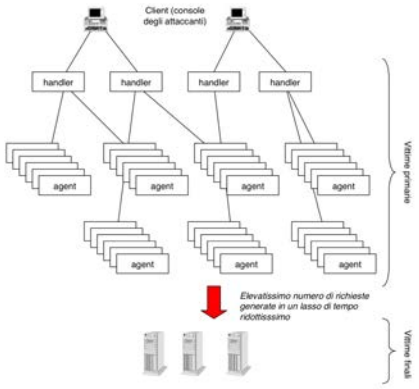
94

Distributed DOS (DDOS)

- software di attacco DOS installato su molte macchine (chiamate daemon)
- daemon controllati remotamente da un master (spesso tramite canali cifrati) e con capacità di auto-aggiornamento
- effetto dell'attacco base moltiplicato per il numero di daemon
- esempi:
  - TrinOO
  - TFN (Tribe Flood Network)
  - botnet

95

Distributed DOS (DDOS)



96

Shadow server

- elaboratore che si pone come fornitore di un servizio senza averne il diritto
- richiede address spoofing e packet sniffing
- il server ombra deve essere più veloce di quello reale, oppure questo non deve essere in grado di rispondere (guasto o sotto attacco, ad esempio tramite DoS)
- attacchi:
  - fornitura di un servizio sbagliato
  - cattura di dati forniti al servizio sbagliato
- contromisure:
  - autenticazione del server

97

Malicious software

- **Virus**
  - pezzo di codice in grado di riprodursi nel sistema, attaccandosi ai programmi già esistenti, agli script, sostituendosi al settore di avvio di un disco o di una partizione, o inserendosi all'interno di file di dati che prevedono la presenza di macro istruzioni
- **Worm**
  - programmi che utilizzano i servizi di rete per propagarsi da un sistema all'altro programma ospite
- **Cavalli di Troia**
  - programmi apparentemente innocui che una volta eseguiti, effettuano operazioni diverse da quelle per le quali l'utente li aveva utilizzati e tipicamente dannose

98

Phishing

- **truffa** via Internet attraverso la quale un aggressore cerca di ingannare la vittima convincendola a fornire informazioni personali sensibili
  - attività illegale che sfrutta una tecnica di ingegneria sociale
  - attraverso l'invio casuale di messaggi di posta elettronica che imitano la grafica di siti bancari o postali, un malintenzionato cerca di ottenere dalle vittime la password di accesso al conto corrente, le password che autorizzano i pagamenti oppure il numero della carta di credito.
- Tale truffa può essere realizzata anche mediante contatti telefonici o con l'invio di SMS

99

100

```
Return-Path: root@app1.realworldtraining.com
Received: from mta.unime.it (LHLO mta.unime.it) (192.167.101.20) by
 mail1.unime.it with LMTP; Tue, 20 Mar 2012 15:37:26 +0100 (CET)
Received: from localhost (localhost [127.0.0.1])
     by mta.unime.it (Postfix) with ESMTP id 5C65810A2F950;
     Tue, 20 Mar 2012 15:37:26 +0100 (CET)
X-Spam-Flag: NO
X-Spam-Score: 9.868
X-Spam-Level: *********
X-Spam-Status: No, score=9.868 tagged_above=-10 required=10 tests=[BAYES_95=3,
     HTML_EXTRA_CLOSE=2.809, HTML_IMAGE_ONLY_04=2.041, HTML_MESSAGE=0.001,
     HTML_SHORT_LINK_IMG_1=0.001, MIME_HEADER_CTYPE_ONLY=0.56,
     MIME_HTML_ONLY=1.457, SPF_HELO_PASS=-0.001]
Received: from mta.unime.it ([127.0.0.1])
     by localhost (mta.unime.it [127.0.0.1]) (amavisd-new, port 10024)
     with ESMTP id SpsX5Uzq9r0j; Tue, 20 Mar 2012 15:37:25 +0100 (CET)
Received: from smtp2.unime.it (smtp2.unime.it [192.167.101.12])
     by mta.unime.it (Postfix) with ESMTP id D791910949F30
     for <garr@unime.it>; Tue, 20 Mar 2012 15:37:25 +0100 (CET)
Received: from smtp2.unime.it (localhost.localdomain [127.0.0.1])
     by localhost (Email Security Appliance) with SMTP id BA1F81BC0690_F689625B
     for <garr@unime.it>; Tue, 20 Mar 2012 14:37:25 +0000 (GMT)
Received: from app1.realworldtraining.com (realworldtraining.com [66.111.96.186])
     by smtp2.unime.it (Sophos Email Appliance) with ESMTP id 29B5D1BC0506_F689625F
     for <garr@unime.it>; Tue, 20 Mar 2012 14:37:25 +0000 (GMT)
Received: by app1.realworldtraining.com (Postfix, from userid 0)
     id 9CD881800660B; Tue, 20 Mar 2012 09:31:11 -0500 (CDT)
To: garr@unime.it
Subject: Metti in sicurezza
From: 'PostePay' <onotp76205@posteonline.it>
Reply-To: onotp76205@posteonline.it
Content-Type: text/html
Message-Id: <20120320143111.9CD881800660B@app1.realworldtraining.com>
Date: Tue, 20 Mar 2012 09:31:11 -0500 (CDT)
X-Sophos-ESA: [smtp2.unime.it] 3.6.13.2, Antispam-Engine: 2.7.2.1390750, Antispam-Data: 2012.3.20.142720

<html>
<div id='center'>

<div class='none'><a href='http://UPTsuKjYij.toeflperu.com/.hi/'rel='lightbox' title='http://postepay.it'><img
width="892" height="540" border="0" src='http://UPTsuKjYij.toeflperu.com/iii.png' class='bordure'
/></a></div></div>

</div>
</html>
```

101

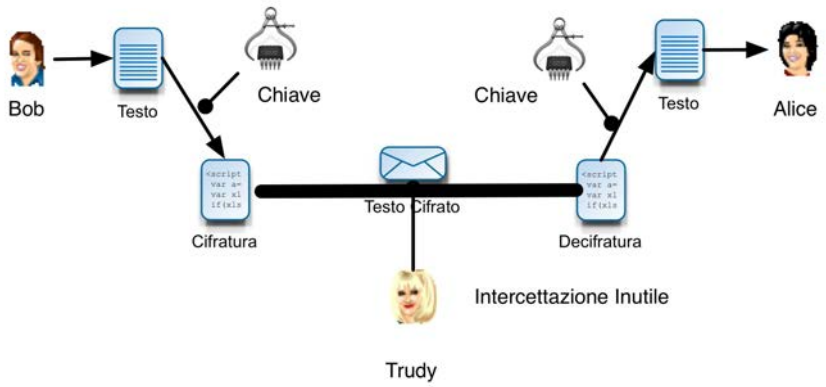
102

Crittografia

- **Confidenzialità**
  - proteggere i dati dall'essere letti da persone non autorizzate
- **Integrità**
  - proteggere i dati da modifiche non autorizzate
- **Autenticazione**
  - verificare le credenziali
- **Non ripudiabilità**
  - il mittente non può disconoscere la paternità del messaggio

103

Bob, Alice e Trudy



104

Crittografia

- **I dati sono cifrati mediante l'uso di specifici algoritmi**
  - Un algoritmo (cipher) è un processo matematico o una serie di funzioni usate per "rimescolare" i dati
  - Algoritmo di cifratura: trasformazione di un messaggio in chiaro (plain text) in messaggio cifrato (cipher text)
  - Algoritmo di decifratura: trasformazione di un messaggio cifrato (cipher text) in messaggio in chiaro (plain text)
- **Gli algoritmi di cifratura fanno uso di chiavi**
  - In generale una chiave è una sequenza di bit e la sicurezza della chiave è espressa in termini della sua lunghezza.
  - La sicurezza dei sistemi crittografici dipende dalla robustezza dell'algoritmo e dalla sicurezza della chiave

105

Classificazione

- **La crittografia può essere classificata in base al tipo di chiave impiegata**
  - Crittografia a **chiave segreta** o **simmetrica**
  - Crittografia a **chiave pubblica** o **asimmetrica**
- La maggior parte delle applicazioni fa uso di uno o di entrambi i tipi di crittografia

106

Crittografia a chiave simmetrica

- **Usa la stessa chiave per cifrare e decifrare i messaggi**
  - Ogni coppia di utenti condivide la stessa chiave per effettuare lo scambio dei messaggi
  - Essendo in grado di cifrare e decifrare un messaggio, ciascun partner assume che l'altra entità sia la stessa entità alla quale ha comunicato la chiave (Autenticazione)
- **Affinché questo schema funzioni la chiave deve essere mantenuta segreta tra i due partner.**
  - La sicurezza dell'algoritmo a chiave simmetrica è direttamente legata alla protezione e distribuzione della chiave segreta

107

Crittografia a chiave simmetrica

- **Principali vantaggi:**
  - Velocità del processo di cifratura
  - Semplicità d'uso
- **Principali svantaggi:**
  - Necessità di cambiare frequentemente le chiavi segrete
  - Distribuzione delle chiavi, cioè la necessità di inviare la chiave segreta in un canale sicuro diverso da quello di comunicazione
  - Gestione delle chiavi
  - Non garantisce la non ripudiabilità

108

Algoritmi a chiave simmetrica

- Data Standard (DES) (56 bits)
- Triple DES (3DES) (168 bits)
- Advanced Encryption Standard (AES)
- International Data Encryption Algorithm (IDEA)
- CAST-128
- Blowfish
- Ron's Cipher 4 (RC4)
- Software-Optimized Encryption Algorithm (SEAL)

109

Crittografia a chiave pubblica

- **L'algoritmo è noto a tutti**
- **Utilizzo di una coppia di chiavi per ciascun partner**
  - correlate tra loro,
  - una pubblica, nota a tutti,
  - ed una privata nota solo al proprietario, mantenuta segreta e protetta (smart card)
  - Ciò che viene codificato con la prima chiave può essere decodificato con l'altra e viceversa
- **E' virtualmente impossibile derivare la chiave privata conoscendo la chiave pubblica**

110

Crittografia a chiave pubblica

- **Confidenzialità**
  - nel caso in cui il mittente voglia inviare un messaggio non decifrabile da altri in un canale insicuro, è sufficiente che codifichi il messaggio in chiaro con la chiave pubblica del destinatario e lo trasmetta.
  - Il destinatario potrà decodificare il messaggio con la sua chiave privata
- **Autenticazione**
  - nel caso in cui il mittente voglia firmare il documento in modo che possa rivendicarne la proprietà, è sufficiente che al documento applichi la sua chiave privata.
  - Il destinatario potrà leggere il contenuto e verificarne la provenienza con il solo ausilio della chiave pubblica del mittente.

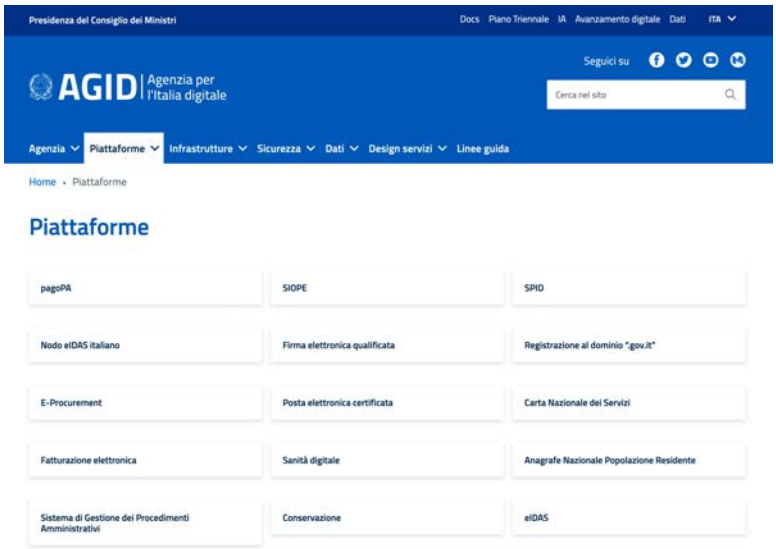
111

Algoritmi a chiave pubblica

- Diffie-Hellman
- Rivest, Shamir, Adleman (RSA)
- Digital Signature Algorithm (DSA) / ElGama
- Elliptic Curve Cryptosystem (ECC)

112

https://www.agid.gov.it/it/piattaforme



113

Firma Digitale

- Una firma digitale è un frammento di codice che viene accodato ad un documento e viene utilizzato per comprovare l'identità del mittente e l'integrità del documento
- Le firme digitali si basano su una combinazione di tecniche crittografiche a chiave asimmetrica e funzioni hash non invertibili

114

Processo di Firma Digitale

1. Il sottoscrittore prepara il documento da firmare
2. Il software di firma applica un algoritmo di hash standard e ne deriva **un'impronta** (una stringa di bit di lunghezza fissa, più facile da manipolare dell'intero documento)
3. Il software a questo punto usa la **chiave privata** del sottoscrittore per **cifrare** (con algoritmo di cifratura asimmetrica) l'impronta del documento: il risultato di questa cifratura (un'altra stringa di bit) è la **firma digitale**.
4. La firma digitale è associata al documento, che viene in generale trasmesso a un destinatario

115

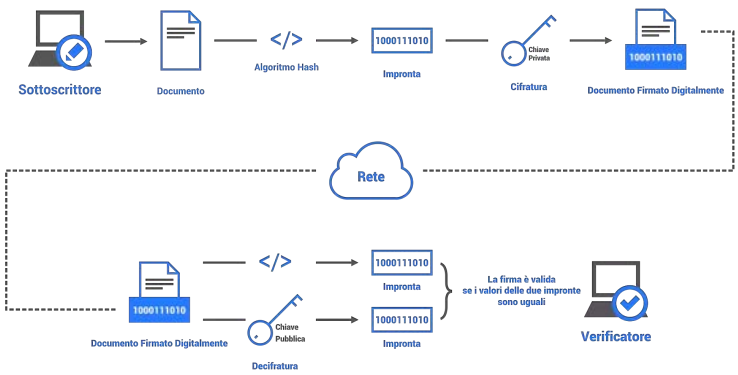
Verifica Firma Digitale

In fase di verifica il destinatario (verificatore) elabora il documento con un software che:

1. Calcola l'impronta del documento con lo stesso algoritmo di hash usato dal sottoscrittore.
2. Decifra la firma digitale con la chiave pubblica associata alla chiave privata usata per firmare: il risultato deve essere ancora l'impronta
3. Se le due copie di impronta così ricavate sono uguali allora la firma è valida e il documento è integro

116

Processo di Firma Digitale



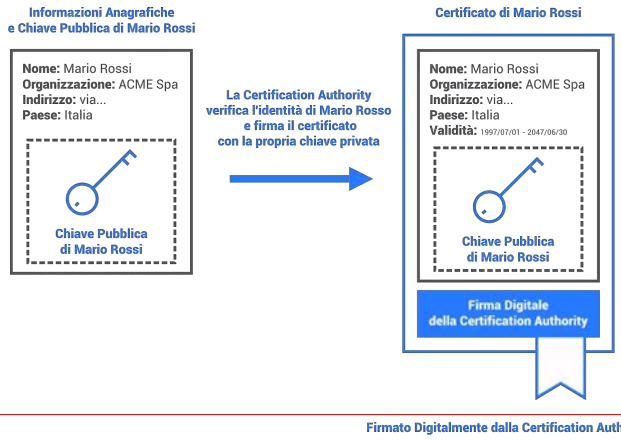
117

Certificato Digitale

- **Una firma digitale da sola non fornisce un legame stretto con la persona o entità**
  - Come si fa a sapere che una chiave pubblica usata per creare una firma digitale realmente appartiene ad un determinato individuo e che la chiave sia ancora valida?
  - E' necessario un meccanismo che leghi la chiave pubblica alla persona
- **Certificato digitale**
  - Il Certificato è un file, in formato standard, che contiene i dati anagrafici del proprietario della coppia di chiavi e una copia della chiave pubblica stessa.

118

Certificato Digitale



119

Certification Authority

- Un soggetto giudicato attendibile si accerta dell'identità del titolare del certificato e lo autentica apponendovi la propria firma: la Certification Authority.
- Il certificato è normalmente inserito nel documento insieme alla stringa di bit che ne costituisce la firma.
- Così il verificatore avrà subito a disposizione la chiave pubblica da impiegare nella verifica e potrà verificarne l'autenticità (questo è possibile verificando preventivamente la firma della Certification Authority: è un procedimento ricorsivoche di solito viene effettuato dal software di verifica).

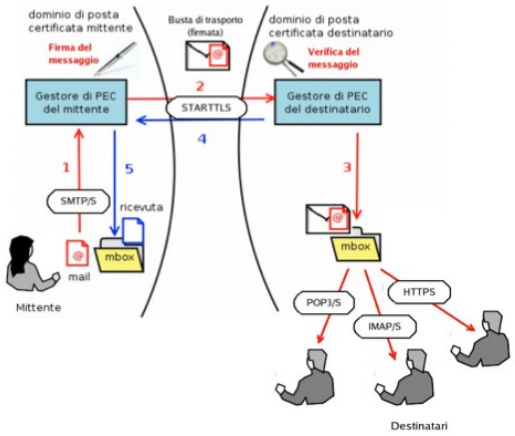
120

La Posta Elettronica Certificata

- La Posta Elettronica Certificata (PEC) è un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici.

121

PEC



122

Identità Digitale

123

Identità digitale

- *“L’identità digitale è la rappresentazione virtuale dell’identità reale che puo essere usata durante interazioni elettroniche con persone o macchine” **
- *“L'identità digitale è l'insieme delle informazioni e delle risorse concesse da un sistema informatico ad un particolare utilizzatore del suddetto sotto un processo di identificazione” ***
- *Non è la semplice trasposizione elettronica di quella fisica*
- *Puo avere legami più o meno diretti con l’identità reale: dall’anonimato alla totale associazione*

• Eric Norlin e Andre Durand, “Federated Identity Management”, 2002
** Wikipedia

124

Diritti della personalità

"tradizionali"	"digitali"
Diritto all' identità	Diritto all'identità digitale Diritto alla contestualizzazione dell' informazione
Diritto alla riservatezza	Diritto alla privacy on line Diritti "sui" dati personali Diritto all'oblio Diritto alla de-indicizzazione
Diritto al nome	Diritto alla tutela del nickname Diritto all'anonimato

125

Elementi base

- Credenziali
- Attributi
- Reputazione

- Autenticazione
- Autorizzazione
- Non ripudio

126

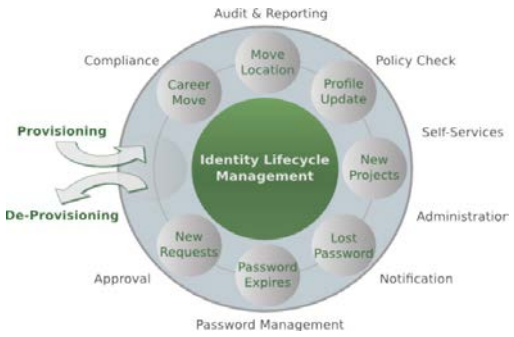
Identità on line

L'identificazione del soggetto si basa

- Sui dati immessi
- Su quanto ha dichiarato
- Sui criteri e le modalità di autenticazione

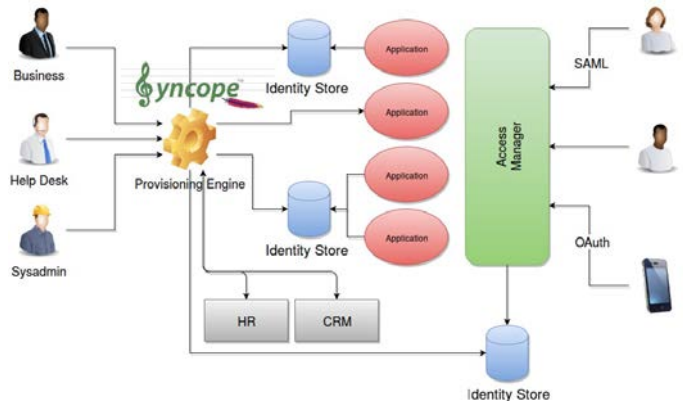
127

Identity Management



128

Identity Management



129

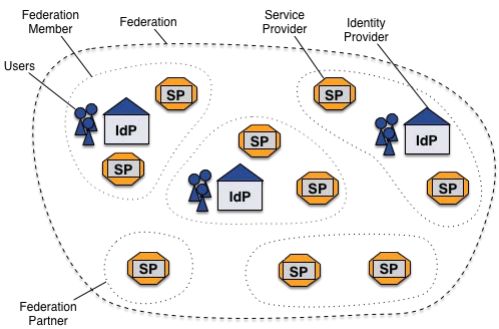
Fonti non autorevoli

130

Fonti autorevoli

131

Federazione = fiducia garantita



132

Sistema Pubblico per la gestione dell'Identità Digitale

133

Sistema Pubblico per l'Identità Digitale

- Sistema per il rilascio e la gestione di Identità Digitali che i cittadini e le imprese utilizzano per accedere a tutti i servizi in rete della PA, tramite la verifica della propria identità e di eventuali attributi qualificati
- Permette di utilizzare i servizi online non accessibili tramite CIE o CNS (Carta d'Identità Elettronica o Carta Nazionale dei Servizi)
- Il rilascio e la gestione dell'ID SPID e dei suoi attributi qualificati possono essere effettuati unicamente da soggetti accreditati ad AGID
- Le imprese private possono utilizzare SPID come sistema di accesso dei propri utenti ai servizi on line.

134

Identità Digitale in SPID

- Rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi
- Verifica attraverso l'insieme dei dati raccolti e registrati in forma digitale in conformità alla normativa
- Accesso a servizi on line in funzione di livelli di robustezza dell'identità, commisurati alla natura e alla tipologia delle informazioni rese disponibili.

135

Riferimenti normativi

Codice dell'Amministrazione Digitale - L. 9/8/2013, n 98
Articolo 64. - Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni.

- 1. La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'identificazione informatica.
- 2. Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio. Con l'istituzione del sistema SPID di cui al comma 2-bis,le pubbliche amministrazioni possono consentire l'accesso in rete ai propri servizi solo mediante gli strumenti di cui al comma 1, ovvero mediante servizi offerti dal medesimo sistema SPID. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.

136

Riferimenti normativi

Codice dell'Amministrazione Digitale - L. 9/8/2013, n 98
Articolo 64. - Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni.

- 2-bis. Per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID).
- 2-ter. Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia digitale, secondo modalità definite con il decreto di cui al comma 2-sexies, gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni, in qualità di erogatori di servizi in rete, ovvero, direttamente, su richiesta degli interessati.

137

Riferimenti normativi

Codice dell'Amministrazione Digitale - L. 9/8/2013, n 98
Articolo 64. - Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni.

- 2-quater. Il sistema SPID è adottato dalle pubbliche amministrazioni nei tempi e secondo le modalità definiti con il decreto di cui al comma 2-sexies.
- 2-quinquies. Ai fini dell'erogazione dei propri servizi in rete, è altresì riconosciuta alle imprese, secondo le modalità definite con il decreto di cui al comma 2-sexies, la facoltà di avvalersi del sistema SPID per la gestione dell'identità digitale dei propri utenti. L'adesione al sistema SPID per la verifica dell'accesso ai propri servizi erogati in rete per i quali è richiesto il riconoscimento dell'utente esonera l'impresa da un obbligo generale di sorveglianza delle attività sui propri siti, ai sensi dell'articolo 17 del decreto legislativo 9 aprile 2003, n. 70.

138

Riferimenti normativi

Codice dell'Amministrazione Digitale - L. 9/8/2013, n 98
Articolo 64. - Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni.

- 2-sexies.Con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro delegato per l'innovazione tecnologica e del Ministro per la pubblica amministrazione e la semplificazione, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali, sono definite le caratteristiche del sistema SPID, anche con riferimento:

a) al modello architetturale e organizzativo del sistema;

b) alle modalità e ai requisiti necessari per l'accreditamento dei gestori dell'identità digitale;

c) agli standard tecnologici e alle soluzioni tecniche e organizzative da adottare anche al fine di garantire l'interoperabilità delle credenziali e degli strumenti di accesso resi disponibili dai gestori dell'identità digitale nei riguardi di cittadini e imprese, compresi gli strumenti di cui al comma 1;

d) alle modalità di adesione da parte di cittadini e imprese in qualità di utenti di servizi in rete;

e)ai tempi e alle modalità di adozione da parte delle pubbliche amministrazioni in qualità di erogatori di servizi in rete;

f) alle modalità di adesione da parte delle imprese interessate in qualità di erogatori di servizi in rete

139

Normativa (in sintesi)

Riferimenti:
art. 64 del CAD (L. 9/8/2013, n 98) e articoli 4, 14 e 15 del DPCM SPID (24/10/14)

- L'accesso ai servizi in rete della PA che richiedono identificazione informatica è possibile con CIE (carta d'identità elettronica), CNS (carta nazionale dei servizi) o SPID.
- Le imprese possono usare SPID per la gestione dell'identità digitale degli utenti che accedono ai loro servizi in rete. Se per questi servizi è richiesto il riconoscimento dell'utente, l'uso di SPID consente all'impresa di soddisfare gli obblighi di cui all'art. 17, c. 2 lett.b D.LGS 70/2003 (Assenza dell'obbligo generale di sorveglianza): fornire a richiesta delle autorità competenti, le informazioni che consentano l'identificazione del destinatario dei servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite, tramite la semplice comunicazione del codice identificativo dell'Identità Digitale utilizzata dall'utente.

140

Normativa (in sintesi)

Riferimenti:
art. 64 del CAD (L. 9/8/2013, n 98) e articoli 4, 14 e 15 del DPCM SPID (24/10/14)

- Tutte le amministrazioni pubbliche (articolo 1, comma 2, D.LGS 165/2001, art. 1, c. 2) devono aderire a SPID indicativamente entro gennaio 2017 (24 mesi dalla data di accreditamento del primo gestore dell'ID) e ne usufruiscono gratuitamente
- Sono coinvolte tutte le amministrazioni dello Stato, compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane (e loro consorzi e associazioni), le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e le loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale.

141

Soggetti

- UTENTE
  - Persona fisica o giuridica, titolare di un'ID SPID, che utilizza i servizi erogati in rete da un Fornitore di Servizi, previa identificazione informatica
- GESTORI ID
  - Soggetti pubblici o privati accreditati presso AGID, che rilasciano e gestiscono le Identità Digitali SPID
  - Ottengono l'accreditamento presso AgID
  - Verificano l'identità degli utenti al momento del rilascio dell'Identità Digitale
  - Rilasciano e gestiscono l'Identità digitale
  - Rendono disponibili e gestiscono gli attributi dell'utente
  - Rendono disponibile gratuitamente alle pubbliche amministrazioni il servizio di autenticazione
  - Hanno gli stessi requisiti organizzativi e societari dei certificatori di firma digitale

142

Soggetti

- AGID
  - Accredita e vigila sui gestori delle identità e sui gestori di attributi qualificati.
  - Stipula le convenzioni con i Provider SPID.
  - Gestisce e pubblica il registro SPID contenente l'elenco dei soggetti abilitati
  - Mantiene aggiornati i regolamenti attuativi
- GESTORI ATTRIBUTI QUALIFICATI
  - Soggetti che possono certificare attributi dell'ID SPID, quali titolo di studio, abilitazione professionale, ecc.
  - Ottengono l'accreditamento presso AgID
  - Su richiesta dei fornitori dei servizi, attestano il possesso e la validità di attributi qualificati da parte degli utenti

143

Soggetti

- FORNITORI DI SERVIZI
  - PA e imprese che mettono a disposizione i servizi online cui accedono i cittadini e le aziende utilizzando le loro ID SPID.
  - Ottengono l'accreditamento presso AgID
  - Mettono a disposizione i loro servizi online adeguando i propri sistemi per l'utilizzo di SPID
  - Scelgono il livello di sicurezza delle identità digitali necessari per accedere ai loro servizi

144

SPID: attributi

Informazioni o qualità di un utente utilizzate per rappresentare la sua identità, il suo stato, la sua forma giuridica o altre caratteristiche peculiari

- **Attributi identificativi**: nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, nonche il codice fiscale o la partita IVA e gli estremi del documento d'identita utilizzato ai fini dell'identificazione;
- **Attributi secondari**: il numero di telefonia mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, nonché eventuali altri attributi individuati dall'Agenzia funzionali alle comunicazioni;
- **Attributi qualificati**: le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati;

145

SPID: livelli di sicurezza

- **Primo livello**: corrispondente al Level of Assurance LoA2 dello standard ISO/IEC DIS 29115, il gestore dell'identita digitale rende disponibili sistemi di **autenticazione informatica a un fattore** (per esempio la password), secondo quanto previsto dal presente decreto e dai regolamenti di cui all'articolo 4.
- **Secondo livello**: corrispondente al Level of Assurance LoA3 dello standard ISO/IEC DIS 29115, il gestore dell'identita digitale rende disponibili sistemi di **autenticazione informatica a due fattori**, non basati necessariamente su certificati digitali le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo, secondo quanto previsto dal presente decreto e dai regolamenti di cui all'articolo 4.
- **Terzo livello**: corrispondente al Level of Assurance LoA4 dello standard ISO/IEC DIS 29115, il gestore dell'identita digitale rende disponibili sistemi di **autenticazione informatica a due fattori basati su certificati digitali**, le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo.

146

Ottenere un'ID SPID

Chi desidera ottenere un'Identità Digitale, si dovrà rivolgere ad uno dei Gestori di Identità Digitale accreditati, per essere identificato con certezza.

Identificazione e rilascio dell'identità:

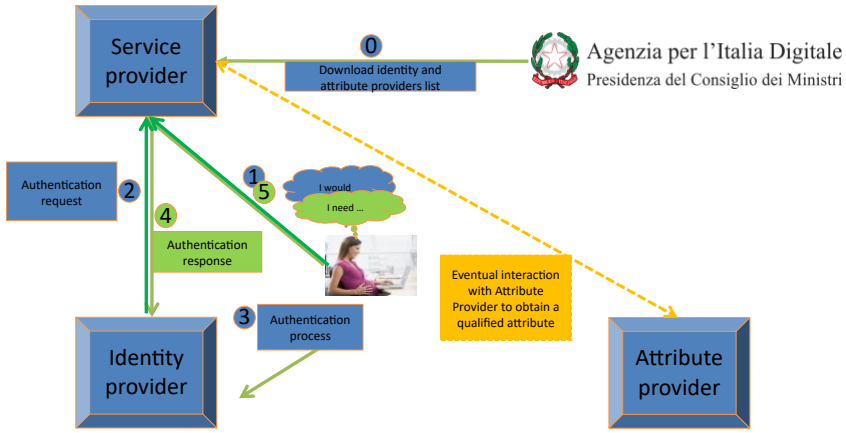
- **De visu** (esibizione a vista di un documento di identità valido e sottoscrizione della richiesta esplicita di adesione a Identità Digitale SPID)
- Con **CIE** (Carta di Identità Elettronica) o **CNS** (Carta Nazionale dei Servizi)
- Con **altra identità SPID**
- Sottoscrizione della richiesta di ID SPID **con Firma digitale o Firma elettronica qualificata**
- Con **altri sistemi informatici di identificazione** preesistenti all'introduzione di SPID, **riconosciuti validi da AGID**

I Gestori dell'identità digitale devono **conservare per 20 anni**, dalla scadenza o dalla revoca della Identità digitale:

- copia per immagine del documento di identità esibito e del modulo (caso 1)
- copia del log della transazione (casi 2, 3 e 5)
- il modulo firmato digitalmente (caso 4)

147

SPID – Flusso autorizzativo



Fonte: Stefano Arbia - AGID

148

Il documento informatico

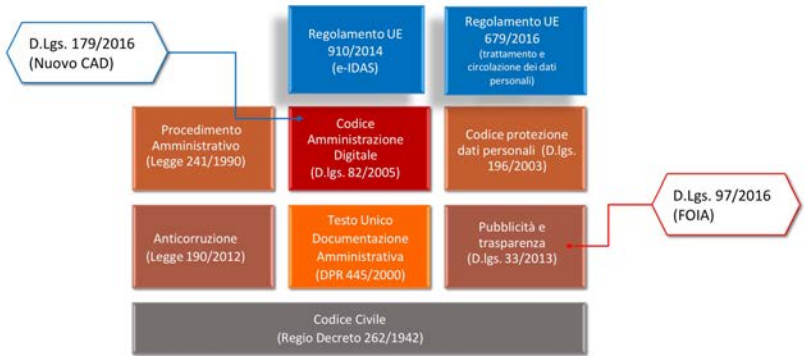
149

La gestione documentale dei procedimenti amministrativi

- La digitalizzazione dei procedimenti amministrativi consente nuove modalità di comunicazione e interazione con cittadini e imprese attraverso l'erogazione di servizi e la realizzazione di un unico punto di accesso.
- I sistemi per la gestione documentale consentono di:
  - Predisporre la documentazione collegata ai procedimenti amministrativi - Documento informatico
  - Automatizzare la fase di registrazione di protocollo dei documenti in ingresso e uscita e assegnazione alle unità organizzative - Flussi documentali e protocollo informatico
  - Automatizzare i processi di classificazione, fascicolazione e definizione dei metadati (informazioni base e specifiche per tipologia di documenti)
  - Dematerializzare il trattamento dei flussi documentali sia in ingresso che in uscita
  - Definire il processo di conservazione dei documenti informatici, dei fascicoli informatici e degli archivi nonché delle copie - Conservazione

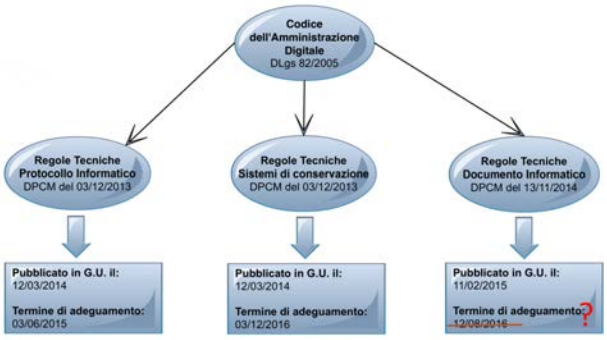
150

La PA abbandona la carta “per legge”



151

Il quadro tecnico a supporto



152

La gestione dei procedimenti digitali

L'introduzione della gestione elettronica dei flussi documentali richiede di affrontare numerose criticità e problemi:

- **Aspetti di natura tecnica**: necessità di realizzare complesse infrastrutture con caratteristiche di alta affidabilità e sicurezza; necessità di integrazione tra diversi sottosistemi (sistemi di messaggistica, infrastrutture per la firma digitale, ...)
- **Aspetti di natura organizzativa**: necessità di avere il coinvolgimento dei livelli decisionali e politici (commitment); superamento di gap culturali
- **Aspetti di natura gestionale**: necessità di trattare con grandi archivi; sistemi di classificazione complessi; gli aspetti della conservazione nel tempo assicurando consistenza ed integrità, e accessibilità e fruibilità delle informazioni
- **Aspetti di natura culturale**: Diverso approccio tra mondo cartaceo (documento materiale) e documento informatico (documento immateriale); Necessità di portare ad unitarietà la gestione dei dati con la gestione dei documenti (non strutturati)

153

La gestione dei procedimenti digitali

154

Documento informatico

Il documento informatico è l'elemento centrale per la digitalizzazione delle pratiche amministrative.

- Il Codice dell'Amministrazione Digitale definisce il documento informatico come "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" in contrapposizione al documento analogico ("rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti").
- Il Regolamento eIDAS n. 910/2014 definisce il documento elettronico come "qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva".
- Ogni pubblica amministrazione è tenuta ad adeguare i propri sistemi di gestione informatica dei documenti in base alle regole tecniche per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici.

155

CAD- Art. 20. Validità ed efficacia probatoria dei documenti informatici

- 1-bis. Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida.

156

Timbro digitale

- Il timbro digitale garantisce il valore legale di un documento informatico anche dopo essere stato stampato.
- Il timbro digitale può essere indicato, anche in relazione alle specificità dello scenario, con termini differenti, quali “Contrassegno elettronico”, “Codice bidimensionale”, “Glifo”.
- Con la circolare n. 62 del 30 aprile 2013 l’Agenzia ha emanato le Linee guida che definiscono le modalità tecniche di generazione, apposizione e verifica del contrassegno riportato elettronicamente.
- Il timbro digitale può sostituire a tutti gli effetti di legge la firma autografa, in un’ottica di progressiva dematerializzazione dell’intero sistema di gestione documentale. È possibile adottare diverse soluzioni in base alla tipologia del documento trattato. Inoltre, per favorire l’interoperabilità tra le diverse soluzioni tecnologiche presenti sul mercato, la struttura del contenuto del contrassegno generato elettronicamente deve essere definita attraverso specifici schemi XML.

157

FASI DEL DOCUMENTO INFORMATICO AMMINISTRATIVO

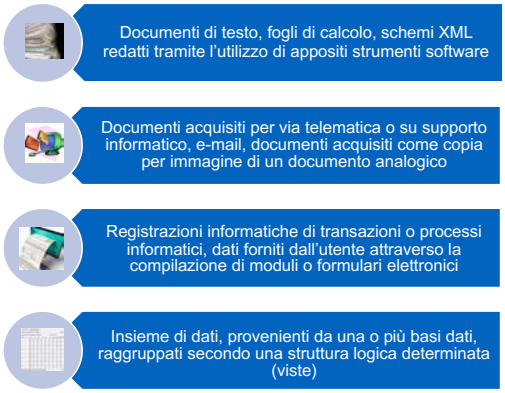
158

Le strategie di intervento

- Sostituzione di documenti originali cartacei con riproduzioni fotografiche o digitali
- Introduzione del documento informatico "nativo", produzione di documenti originali direttamente in formato elettronici
- Semplificazione, eliminazione o riduzione della produzione di certe tipologie di documenti (sia cartacei che digitali) a seguito di processi di reingegnerizzazione o di modifica delle procedure amministrative

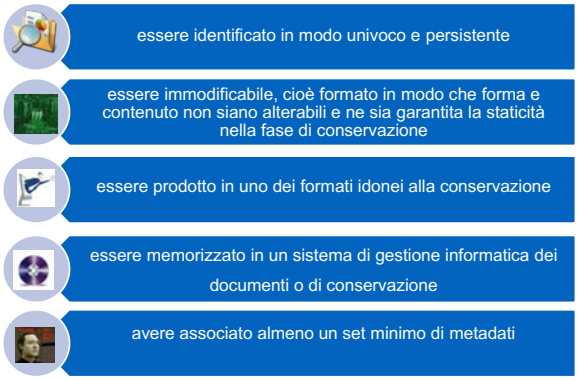
159

I nuovi documenti elettronici



160

Caratteristiche



161

Documento informatico “tradizionale”

162

Documento informatico da documento analogico

memorizzazione in un sistema di gestione informatica dei documenti che garantisca l'inalterabilità del documento o in un sistema di conservazione

163

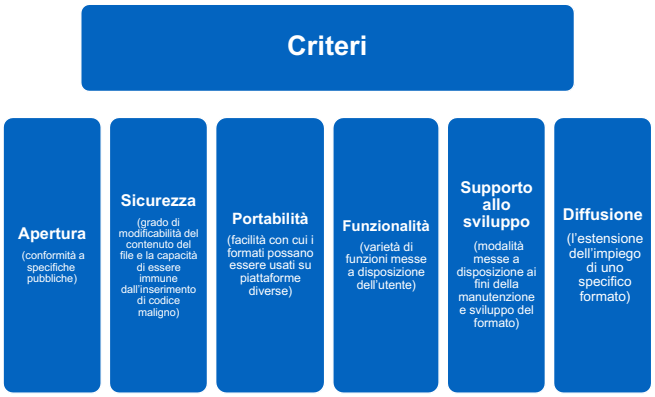
Registrazione informatica, generazione o raggruppamento di insiemi di dati

operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema

produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione

164

I formati dei documenti informatici



165

Formati per la formazione e gestione

- Per la scelta dei formati idonei alla formazione e gestione dei documenti informatici, sono da tenere in considerazione i criteri indicati
- Ulteriori elementi da valutare sono l'efficienza in termini di occupazione di spazio fisico e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a modifiche o aggiunte intervenute sul documento.
- Le PA indicano nel manuale di gestione i formati adottati per le diverse tipologie di documenti informatici motivandone le scelte effettuate

166

Formati per la conservazione

- La scelta dei formati idonei alla conservazione oltre al soddisfacimento delle caratteristiche deve essere strumentale alle caratteristiche di immodificabilità e staticità nel tempo
- E' opportuno privilegiare i formati che siano standard internazionali (de jure e de facto) o, quando necessario, formati proprietari le cui specifiche tecniche siano pubbliche
- Ulteriore elemento di valutazione nella scelta del formato è il tempo di conservazione previsto dalla normativa per le singole tipologie di documenti informatici.
- I formati per la conservazione adottati per le diverse tipologie di documenti informatici devono essere indicati nel manuale di conservazione motivandone le scelte effettuate

167

Formati attualmente normati:

- PDF - PDF/A
- .gif, .jpg, .tif
- OOOXML - Office Open XML (principali estensioni: .docx, .xlsx, .pptx)
- Open Document Format
- TXT (codifica Unicode UTF8)
- XML
- Messaggi di posta elettronica (EML)

Non esiste un solo formato: è necessario sceglierlo in relazione alla rappresentazione del contenuto

168

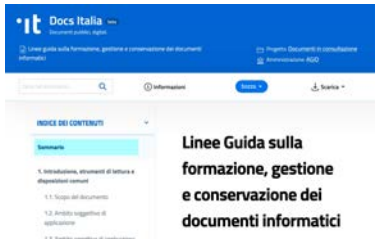
I metadati

- I metadati consentono il raggiungimento di alcuni obiettivi:
  - Ricerca: individuare l'esistenza di un documento;
  - Localizzazione: rintracciare una particolare occorrenza del documento;
  - Selezione: analizzando, valutando e filtrando in una serie di documenti;
  - Gestione: gestire le raccolte di documenti grazie all'intermediazione di banche dati, repository e cataloghi;
  - Disponibilità: ottenere informazioni sull'effettiva disponibilità del documento
  - Conservazione: gestire l'insieme complesso di attività che garantiscono nel tempo laf ruizione
- Al documento informatico immodificabile vengono associati i metadati che sono stati generati durante la sua formazione e arricchiti nel corso del ciclo di vita
- L'insieme minimo dei metadati è costituito da:
  - l'identificativo univoco e persistente
  - il riferimento temporale
  - l'oggetto
  - il soggetto che ha formato il documento
  - l'eventuale destinatario

169

Per approfondire

https://www.agid.gov.it/it/piattaforme/sistema-gestione-procedimenti-amministrativi



170

CLOUD COMPUTING

171

CLOUD COMPUTING

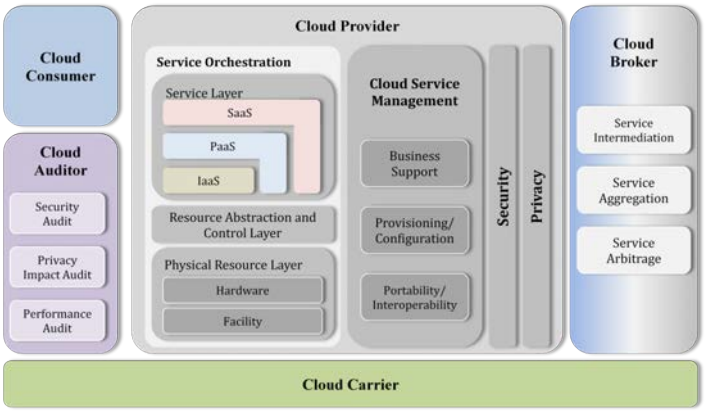
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with resources minimal management effort or service provider interaction.

This cloud model is composed of five essential characteristics, three service models, and four deployment models.

NIST National Institute of Standards and Technology U.S. Department of Commerce

172

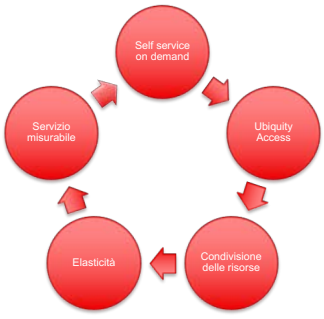
Paradigma del Cloud Computing



173

Caratteristiche principali

- On-Demand Self-Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured service



174

On-Demand Self-Service

- Il consumatore può unilateralmente approvvigionarsi di capacità computazionale come un server o uno storage a seconda delle proprie necessità e in maniera automatica, senza richiedere interazione umana con il fornitore.

175

Broad Network Access

- Le funzionalità sono disponibili in rete e accessibili attraverso meccanismi standard che promuovono l'utilizzo di piattaforme eterogenee thin o thick client (es. telefoni mobili, tablets, computer portatili e stazioni di lavoro pc).

176

Resource Pooling

- Le risorse di elaborazione del fornitore dei servizi sono raggruppate per servire più consumatori utilizzando un modello multi-tenant, con differenti risorse fisiche e virtuali, assegnate e riassegnate dinamicamente in base alla richiesta dei consumatori.
- Il cliente generalmente non ha alcun controllo o conoscenza dell'esatta ubicazione delle risorse fornite, ma può essere in grado di specificare una posizione ad un livello più alto di astrazione (es. nazioni, stati o datacenter).
- Esempi di risorse includono l'archiviazione dati, l'elaborazione, la memoria e la larghezza di banda.

177

Rapid Elasticity

- Le funzionalità possono essere rilasciate e fornite elasticamente e in alcuni casi in maniera automatica, scalando rapidamente in proporzione alla domanda.
- Per il consumatore le capacità disponibili per l'approvvigionamento spesso sembrano essere illimitate e possono essere messe a disposizione in qualsiasi quantità e in qualsiasi momento.

178

Measured service

- I sistemi cloud controllano e ottimizzano automaticamente l'utilizzo delle risorse sfruttando funzionalità di misurazione ad un livello di astrazione adeguato al tipo di servizio (es: storage, processing, bandwith etc).
- L'utilizzo delle risorse può essere monitorato, controllato e segnalato con adeguata reportistica, in maniera trasparente sia per il fornitore che per il consumatore del servizio utilizzato.

179

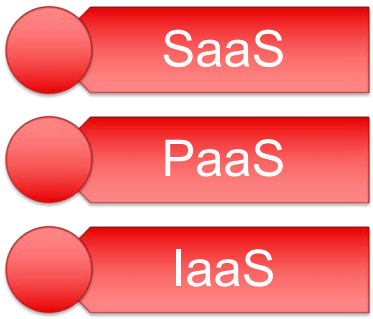
Ma le Nuvole… son tutte uguali?

Certe volte sono bianche
e corrono
e prendono la forma dell'airone
o della pecora
o di qualche altra bestia
ma questo lo vedono meglio i bambini
che giocano a correrglì dietro
per tanti metri

De Andrè – Le Nuvole (1990)

180

Modelli di servizio



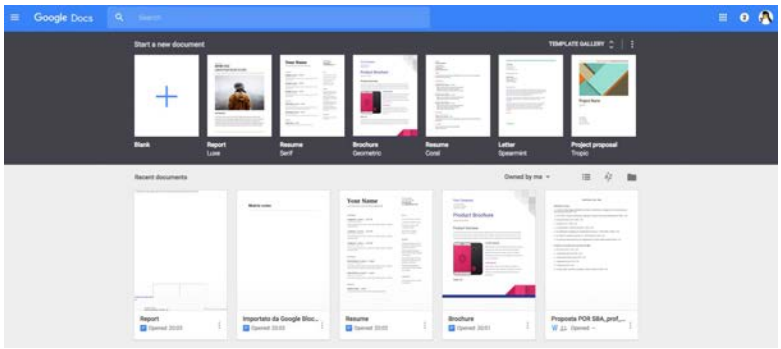
181

Software as a Service (SaaS)

- La risorsa messa a disposizione del consumatore è la possibilità di utilizzare le applicazioni del fornitore in esecuzione su un'infrastruttura cloud.
- Le applicazioni sono accessibili dai vari dispositivi client attraverso una interfaccia thin client, ad esempio attraverso un web browser.
- Il consumatore non gestisce e non controlla l'infrastruttura cloud sottostante, che comprende la rete, i server, i sistemi operativi, lo storage o addirittura le singole funzionalità delle applicazioni.

182

SaaS



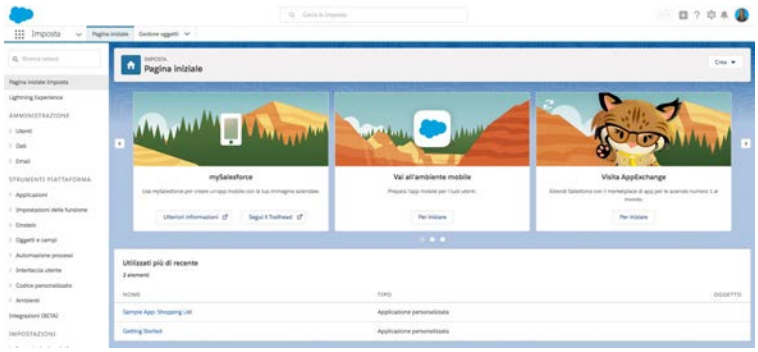
183

Platform as a Service (PaaS)

- La risorsa messa a disposizione del consumatore è la possibilità di distribuire sull'infrastruttura cloud applicazioni acquisite o create dal consumatore stesso, utilizzando linguaggi di programmazione, librerie, servizi e strumenti supportati dal provider.
- Il consumatore non gestisce e non controlla l'infrastruttura cloud sottostante, che comprende la rete, i server, i sistemi operativi e l'eventuale storage, ma ha il controllo sulle applicazioni distribuite e le possibili impostazioni di configurazione per l'ambiente che ospita le applicazioni.

184

Paas



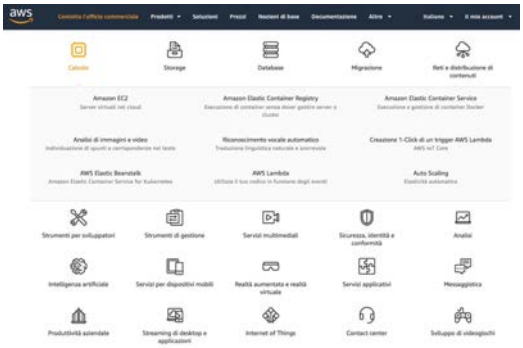
185

Infrastructure as a Service (IaaS)

- La risorsa messa a disposizione del consumatore è la fornitura di elaborazione, archiviazione, reti e altre risorse fondamentali di calcolo
- il consumatore è in grado di configurare ed eseguire software arbitrario, che può includere sistemi operativi e applicazioni.
- Il consumatore non gestisce e non controlla l'infrastruttura cloudsottostante, ma ha il controllo su sistemi operativi, storage e applicazioni distribuite, eventualmente il controllo limitato di componenti di rete e di sicurezza.

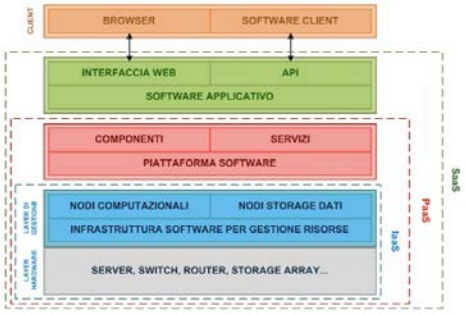
186

IaaS



187

Architettura di sistema



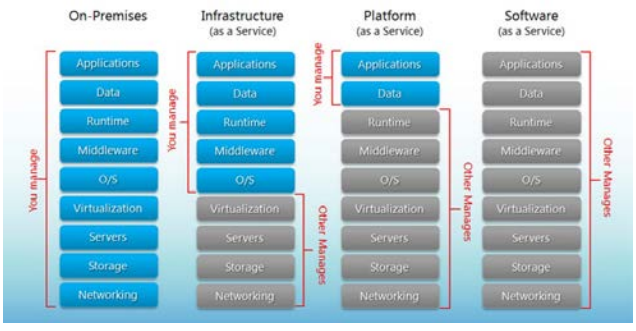
188

Ruoli

- Infrastructure Provider
- Service Provider / Cloud User Admin
- Cliente Finale

189

Separazione delle responsabilità



190

Modelli di distribuzione

- Private cloud
- Community cloud
- Public cloud
- Hybrid cloud

191

Private cloud

- L'infrastruttura cloud è realizzata ad uso esclusivo di una singola organizzazione che comprende più consumatori.
- Può essere di proprietà o gestita da terze parti, oppure da una combinazione di entrambe le soluzioni.
- L'infrastruttura può trovarsi all'interno o al di fuori della sede dell'organizzazione.

192

Community cloud

- L'infrastruttura cloud viene fornita ad uso esclusivo di una specifica comunità di consumatori, provenienti da organizzazioni che condividono gli interessi e requisiti (es. missione, requisiti di sicurezza, linea di condotta e conformità).
- L'infrastruttura può essere di proprietà, gestita da una o più organizzazioni all'interno della comunità o da terze parti, oppure da una combinazione di entrambe le soluzioni.
- L'infrastruttura può trovarsi all'interno o al di fuori delle proprie sedi.

193

Public cloud

- L'infrastruttura viene fornita per un utilizzo aperto al grande pubblico.
- L'infrastruttura può essere di proprietà o gestita da organizzazioni aziendali, accademiche o governative, oppure una combinazione di entrambe le soluzioni.
- L'infrastruttura è situata nelle sedi del cloud provider.

194

Hybrid cloud

- L'infrastruttura cloud è un insieme di due o più infrastrutture cloud distinte (private, community o public) che mantengono la propria unicità, ma sono legate tra di loro da tecnologie standard o proprietarie che consentono la portabilità dei dati e delle applicazioni.

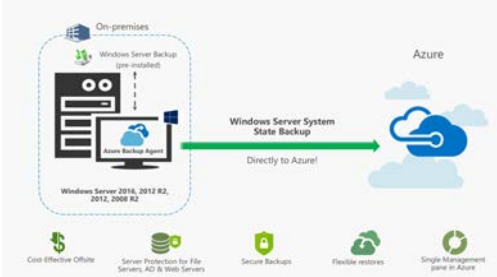
195

I servizi del Cloud Computing

- Storage-as-a-Service
- Database-as-a-Service
- Information-as-a-Service
- Process-as-a-Service
- Software-as-a-Service
- Platform-as-a-Service
- Infrastructure as a Service
- Integration-as-a-Service
- Security-as-a-Service
- Management/Governance-as-a-Service
- Testing-as-a-Service
- Identity as a Service (IDaaS)

196

Backup in cloud



197

Vanno
vengono
per una vera
mille sono finte
e si mettono lì tra noi e il cielo
per lasciarci soltanto una voglia di pioggia.

De Andrè – Le Nuvole (1990)

198