Diritto dell'Informatica

Modulo Tecnico

A.A. 2018-2019

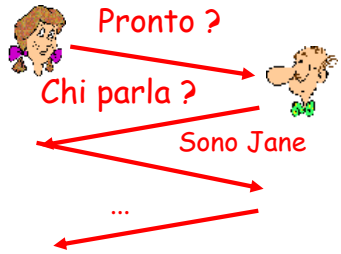
Melchiorre Monaca
melchiorre.monaca@unirc.it

Reti di Telecomunicazione

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

I problemi da risolvere

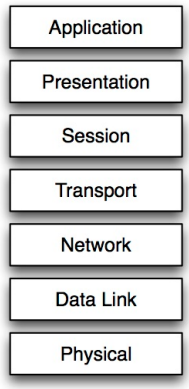
Facciamo una telefonata



Scomponiamo il problema

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

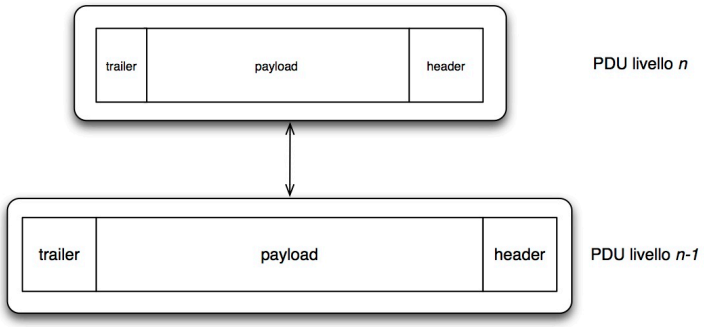
Il modello ISO/OSI



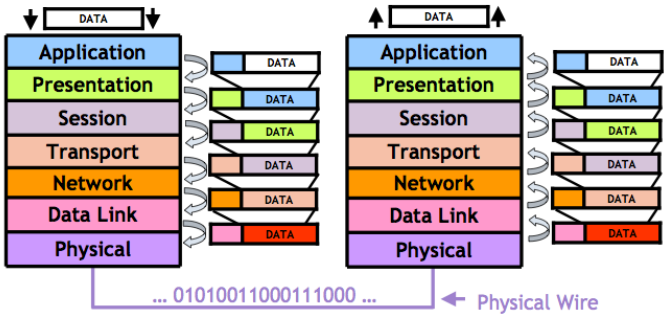
Incapsulamento

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

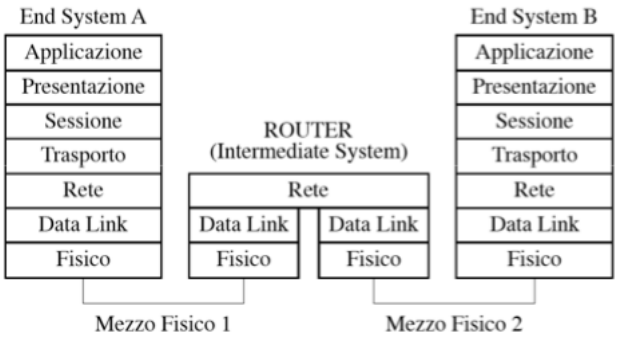
Incapsulamento



Il modello ISO/OSI

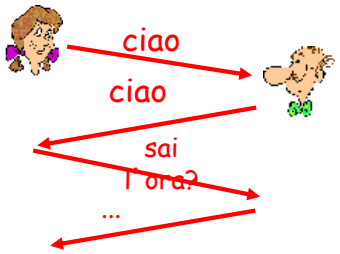


Il modello ISO/OSI



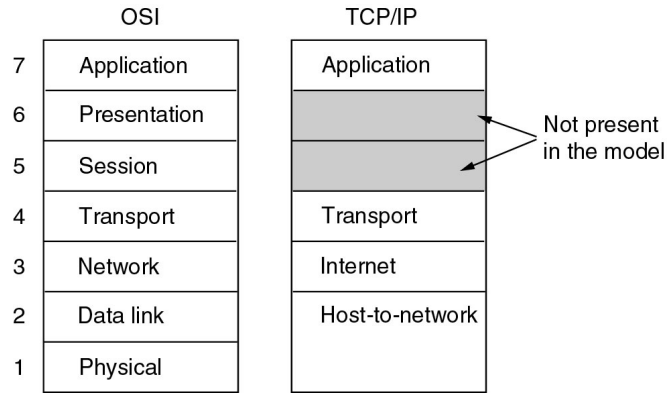
I Protocolli

Conversazione



Connessione di rete

Il TCP/IP



Livello fisico: il mezzo trasmissivo

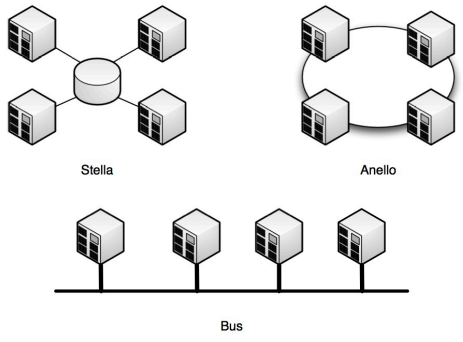
- Cavo elettrico
- Onde radio
- Fibra ottica
- Laser

Classifichiamo

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

Livello fisico: topologia

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

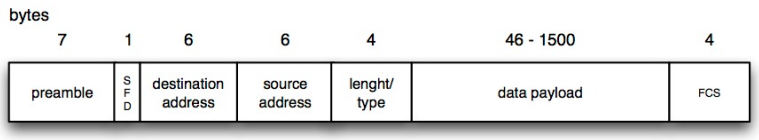


Livello Data Link

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

Livello Data Link: Ethernet

- Frame
- MAC ADDRESS



Livello Network

- Indirizzamento
- Routing
- Internetworking

Livello Network: IP

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

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

Livello Network: IP

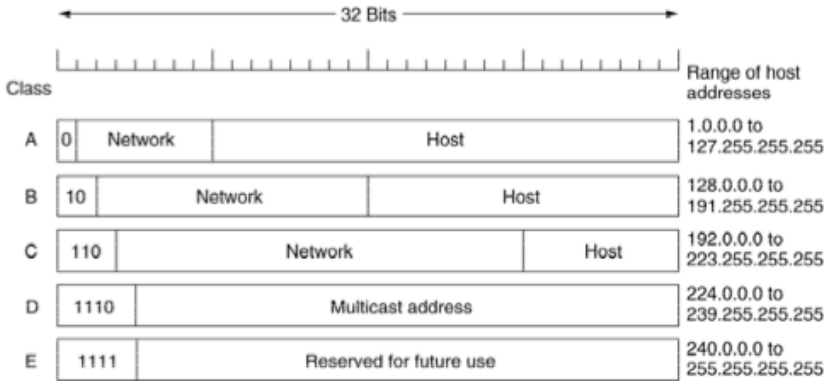
- Ind. host 1.2.3.4 AND netmask 255.255.255.0

  00000001.00000010.00000011.00000100
  AND
  11111111.11111111.11111111.00000000

- Si ottiene indirizzo network 1.2.3.0

  00000001.00000010.00000011.00000000

Livello Network: IP - classi



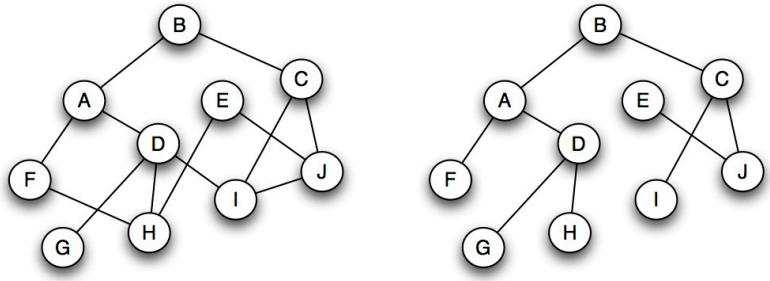
Livello Network: IP – indirizzi privati

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

Livello Network: Routing

- Principio di ottimalità
- Routing statico
- Routing dinamico

Livello Network: Routing



Livello Network: Routing

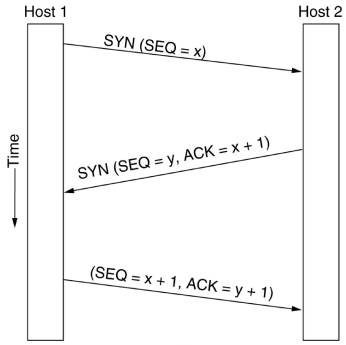
```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, 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
......
```

Livello Transport

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

Livello Transport: TCP

- Three-way handshake



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

Applicazioni

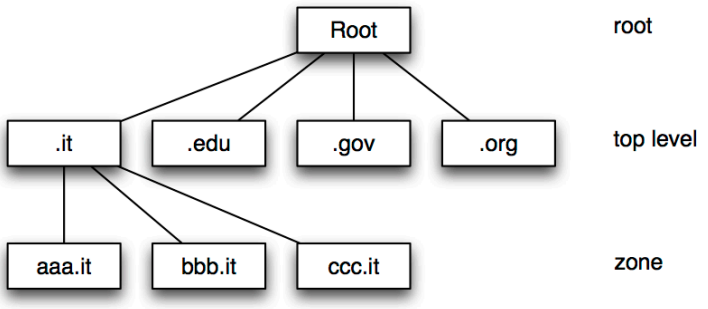
- Dns
- Web
- E-MAIL
- Motori di ricerca
- Content delivery
- Peer to Peer
- Ip Telephony e Videoconferenza
- Chat
- Streaming

DNS – The Domain Name System

- The DNS Name Space
- Resource Records
- Name Servers

The DNS Name Space

A sample of the Internet domain name space.



Resource Records

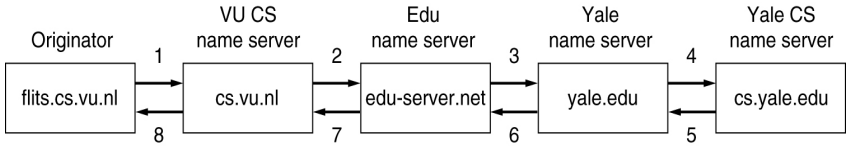
The principal DNS resource records types.

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

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
```

Name Servers (2)



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

Electronic Mail

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

Electronic Mail (2)

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

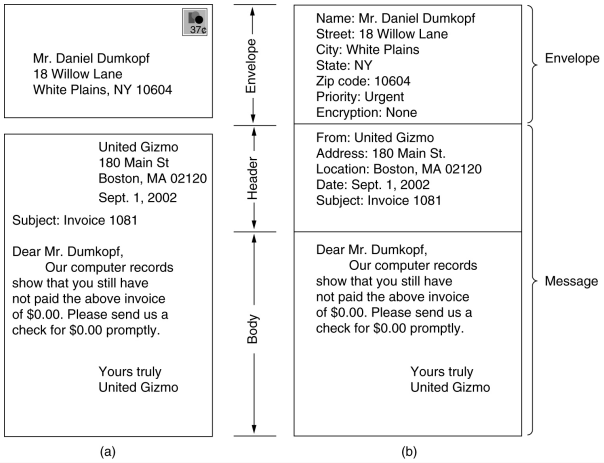
Smiley	Meaning	Smiley	Meaning	Smiley	Meaning
:-)	I'm happy	=|:-)	Abe Lincoln	:+)	Big nose
:-(	I'm sad/angry	=):-)	Uncle Sam	:-))	Double chin
:-|	I'm apathetic	*<:-)	Santa Claus	:-{)	Mustache
;-)	I'm winking	<:-(	Dunce	#:-)	Matted hair
:-(O)	I'm yelling	(-:	Australian	8-)	Wears glasses
:-(*)	I'm vomiting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

E-Mail Architecture and Services

Basic functions

- Composition
- Transfer
- Reporting
- Displaying
- Disposition

The User Agent



Reading E-mail

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 ibJHKOPT9FCg 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
```

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

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

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).

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

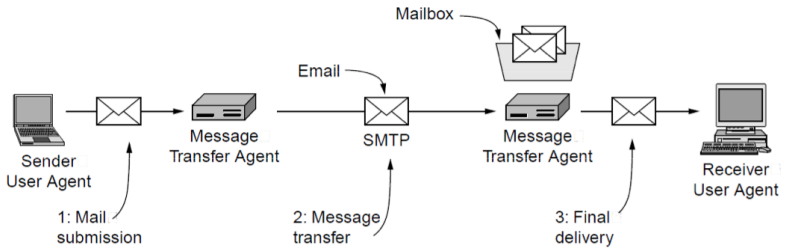
MIME (3)

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

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--
```

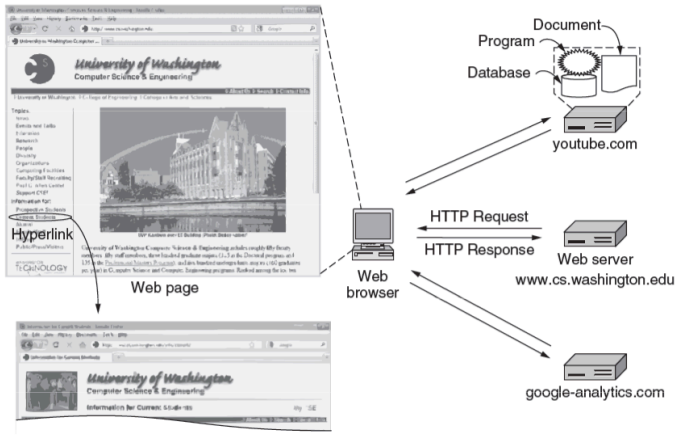
E-mail Delivery



Fetch E-mail

- POP 3
- IMAP

The World Wide Web



URLs – Uniform Resource Locators

Some common URLs.

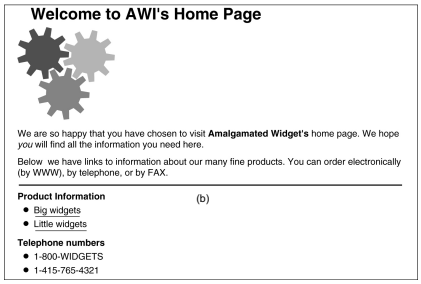
Name	Used for	Example
http	Hypertext (HTML)	http://www.cs.vu.nl/~ast/
ftp	FTP	ftp://ftp.cs.vu.nl/pub/minix/README
file	Local file	file:///usr/suzanne/prog.c
news	Newsgroup	news:comp.os.minix
news	News article	news:AA0134223112@cs.utah.edu
gopher	Gopher	gopher://gopher.tc.umn.edu/11/Libraries
mailto	Sending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

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)

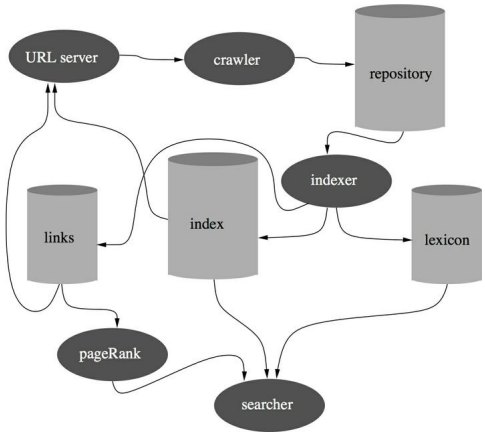


(b)

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

Search Engines



SICUREZZA

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**

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

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

Attacchi alla sicurezza

- **Attacchi passivi**
  - Mapping e port scanning (esplorazione della rete)
  - Sniffing (analisi del traffico)
- **Attacchi attivi**
  - Spoofing (sostituzione)
  - Exploit (sfruttamento di software bug)
  - Malicious software
  - DoS: Denial of Service (negazione del servizio)
  - Phishing

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

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

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**

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)

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

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

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

Da: PostePay <onotp76205@posteonline.it>
Oggetto: Metti in sicurezza
Data: 20 marzo 2012 15:31:11 GMT+01:00
A: garr unime
Rispondi a: onotp76205@posteonline.it

Posteitaliane

Importante

Dal 1° aprile 2012 è necessario attivare il sistema Sicurezza web Postepay per eseguire le operazioni di ricarica Postepay, ricarica telefonica e pagamento bollettini sui siti di Poste Italiane con la tua Postepay.
Per attivare il sistema Sicurezza web Postepay bastano poche, semplici mosse:

- rilascia in qualsiasi Ufficio Postale il tuo numero di telefono cellulare per associarlo alla tua carta Postepay;
- successivamente, abilita la tua carta al nuovo sistema accedendo alla sezione "Sicurezza web" del menù dedicato ai servizi online Postepay.
- **Abilita la tua Postepay al sistema Sicurezza Web**

Scarica la guida (.pdf)*

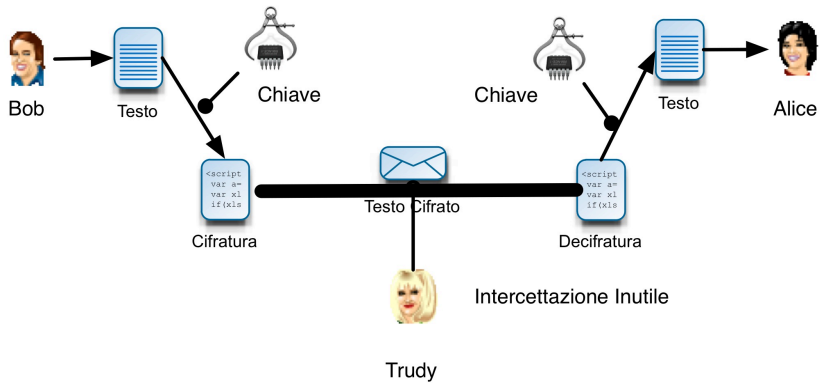
**Per leggere i documenti hai bisogno di Adobe Reader.*
Scarica Adobe Acrobat Reader qui

```
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>
```

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

Bob, Alice e Trudy



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

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

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

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

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)

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**

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.

Algoritmi a chiave pubblica

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

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

Processo di Firma Digitale

- **Creazione di una firma digitale (Mittente "A")**
  - "A" ottiene la coppia chiave pubblica/chiave privata e comunica la propria chiave pubblica al destinatario "B"
  - "A" scrive un messaggio e crea il digest con la funzione hash non invertibile
  - "A" codifica il messaggio con la propria chiave privata ottenendo così la firma digitale
  - "A" appende al documento originale la firma digitale così ottenuta ed invia il tutto al
  - destinatario "B"

Processo di Firma Digitale

- **Creazione di una firma digitale (Destinatario"B")**
  - "B" separa il messaggio ricevuto in documento originale e firma digitale
  - "B" utilizza la chiave pubblica del mittente "A" per decifrare la firma digitale ed ottenere il digest del messaggio originale
  - "B" utilizza il documento originale come input della medesima funzione hash utilizzata da "A" per ottenere il digest del messaggio
  - "B" verifica che le impronte del messaggio siano uguali

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**
  - Un certificato digitale è un messaggio con firma digitale con la chiave privata di un terzo di fiducia (Certification Authority), il quale dichiara che una determinata chiave pubblica appartiene ad una certa persona o entità e ne garantisce nome e caratteristiche
  - I certificati digitali sono il mezzo di distribuzione delle chiavi pubbliche

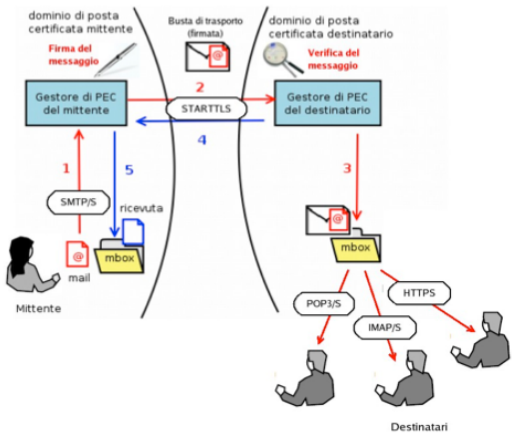
Certification Authority

- **La Certification Authority (CA) è il soggetto terzo di fiducia che avalla la validità di un certificato**
  - Alla CA spetta il compito di raccogliere le richieste, rilasciare e distribuire i certificati, sospenderli o revocarli quando le informazioni in essi contenute non sono più valide
- **Come ottenere la chiave pubblica di un partner dalla CA:**
  - "A" chiede alla CA il certificato digitale di "B"
  - La CA invia ad "A" il certificato di "B" che contiene come firma la chiave pubblica della CA stessa
  - "A" riceve il certificato di "B" e verifica la firma della CA
  - Poiché il certificato di "B" contiene la chiave pubblica, "A" ha ora una copia autenticata della chiave pubblica di "B"

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.

PEC



Identità Digitale

Identità digitale

- *“L’identità digitale è la rappresentazione virtuale dell’identità reale che può 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*
- *Può 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

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

Elementi base

- Credenziali
- Attributi
- Reputazione

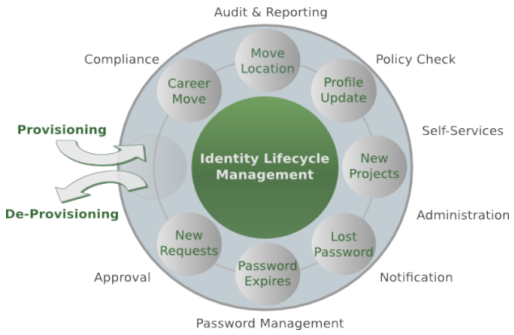
- Autenticazione
- Autorizzazione
- Non ripudio

Identità on line

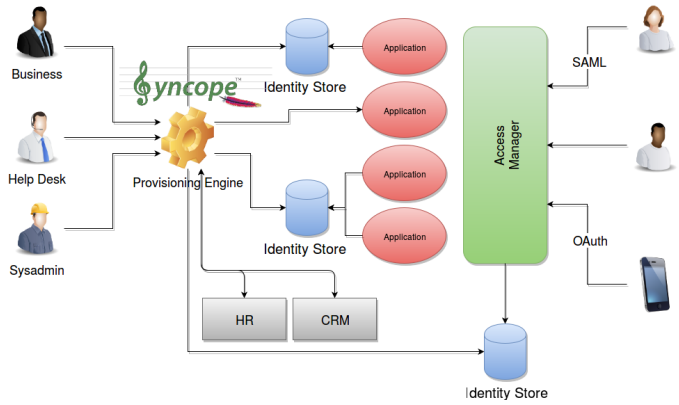
L'identificazione del soggetto si basa

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

Identity Management



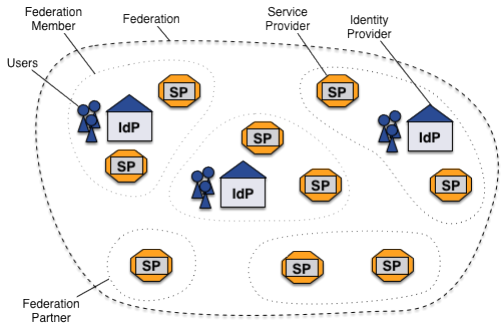
Identity Management



Fonti non autorevoli

Fonti autorevoli

Federazione = fiducia garantita



Sistema Pubblico per la gestione dell'Identità Digitale

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.

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.

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.

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.

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.

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

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.

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.

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

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

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

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;

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.

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.

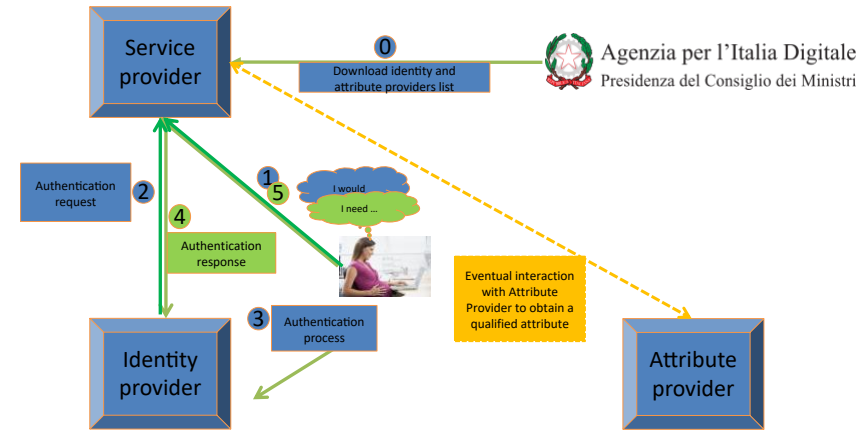
Identificazione e rilascio dell'identità:

- **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)

SPID – Flusso autorizzativo



Fonte: Stefano Arbia - AGID

CLOUD COMPUTING

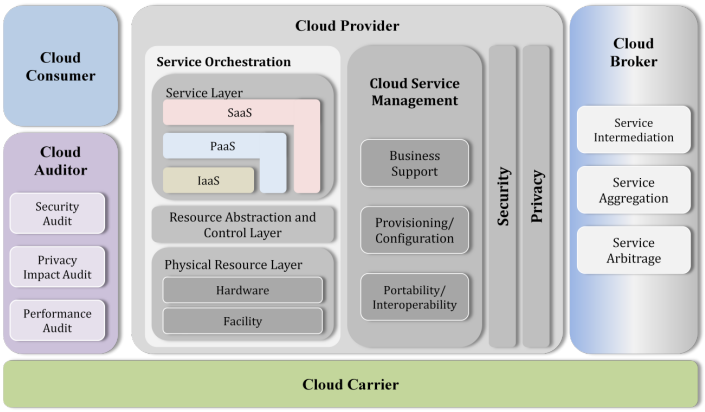
CLOUD COMPUTING

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 witresourcesh minimal management effort or service provider interaction.

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

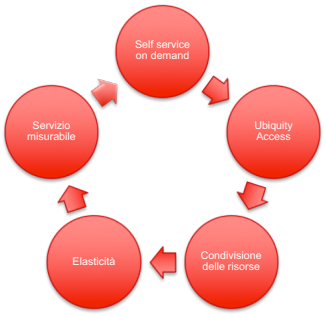
NIST National Institute of Standards and Technology U.S. Department of Commerce

Paradigma del Cloud Computing



Caratteristiche principali

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



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.

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).

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.

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.

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.

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)

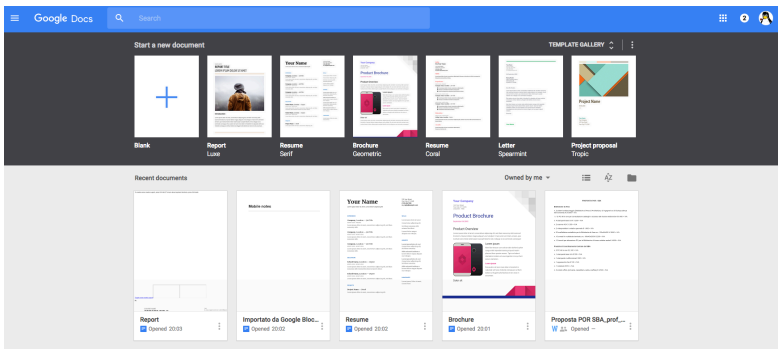
Modelli di servizio

- SaaS
- PaaS
- IaaS

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.

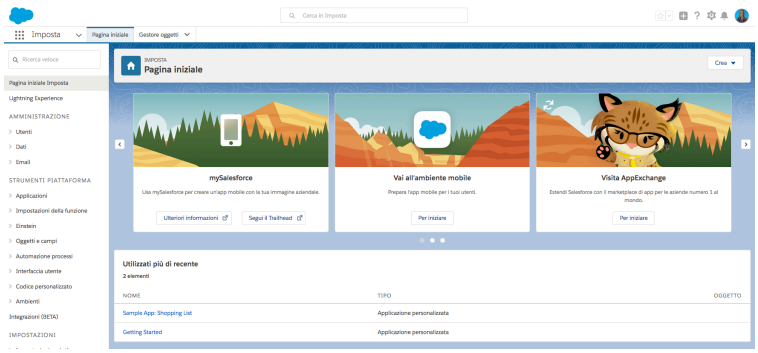
SaaS



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.

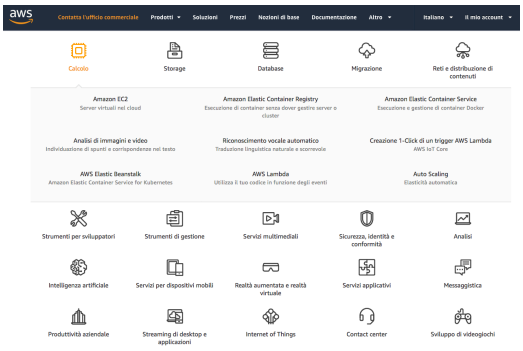
Paas



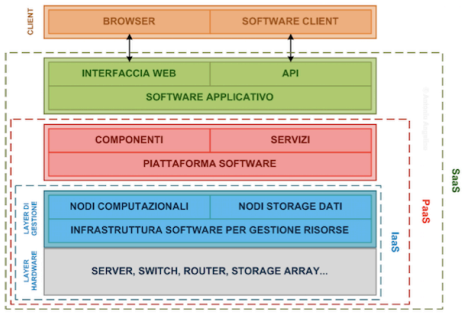
Infrastructure as a Service (IaaS)

- 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.

IaaS



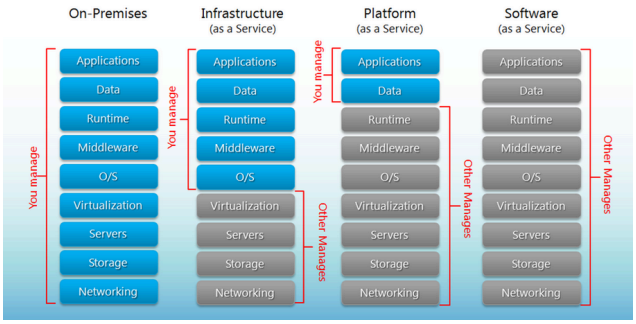
Architettura di sistema



Ruoli

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

Separazione delle responsabilità



Modelli di distribuzione

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

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.

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.

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.

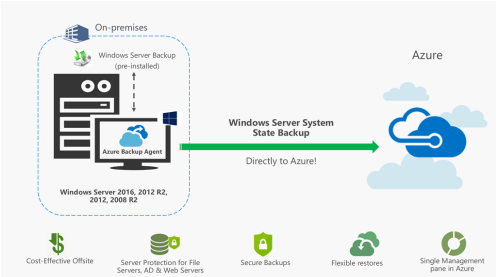
Hybrid cloud

- 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.

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)

Backup in cloud



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)