

**GARR**

The Italian Academic & Research Network



www.garr.it

# Introduzione al Convegno “Dalle password all'identità digitale federata”

Enzo Valente

Primo Convegno IdeM, 30-31 marzo 2009, Uni-Roma3

10110

Consortium  
GARR

# II "GARR"

- L'acronimo **GARR** deriva da "Gruppo per l'Armonizzazione delle Reti della Ricerca".
- Questo Gruppo si e' costituito nel 1987 allo scopo di rappresentare organicamente la comunita' scientifica delle Universita' e degli Enti Pubblici di Ricerca italiani nelle attivita' di realizzazione, gestione, ricerca e utilizzazione delle reti informatiche nei confronti della Commissione Europea e nei confronti delle organizzazioni di Reti di Ricerca gia' esistenti nei paesi culturalmente ed economicamente piu' avanzati.

# Finalita' del GARR

- La comunita' della Ricerca Scientifica e dell'Accademia italiana, si propone i seguenti obiettivi:
  - mantenere il passo con l'Europa in termini di incremento delle prestazioni e adeguamento delle tecnologie (soprattutto per far fronte alle esigenze delle griglie computazionali, dell'insegnamento a distanza, dell'accesso multimediale a biblioteche e musei, della multi-videoconferenza) e a costi contenuti e 'proponibili', a livello nazionale e internazionale;
  - garantire alle sedi universitarie e ai laboratori di ricerca situati nell'Italia meridionale le stesse prestazioni di rete di cui la comunita' scientifica GARR puo' usufruire nell'Italia Centrale e Settentrionale;
  - svolgere un ruolo di rilievo nel bacino del Mediterraneo, sia in termini di cooperazione che di passerella verso l'Europa.

# Finalita' della Rete dell'Universita' e della Ricerca

- strumento per facilitare lo svolgimento della ricerca scientifica ed dell'attivit  accademica,
- la rete dell'Universita' e della Ricerca GARR induce, tra l'altro:
  - sviluppo di nuove tecnologie HW, MW e SW sull'industria del software e delle telecomunicazioni su Internet
  - sviluppo di infrastrutture fisiche (fibre) da parte degli operatori di telecomunicazioni anche in aree di scarsa densita' demografica (vedi area Mediterranea)
  - formazione avanzata di progettisti e tecnici di rete
  - ricerca e sviluppo di nuove tecnologie di rete
  - sviluppo di nuove applicazioni e tecnologie software
  - costante adeguamento alle reti della ricerca mondiali

## Armonizzazione e sinergia tra Università' e Enti di Ricerca

- **1973-1990:** reti indipendenti di CNR, ENEA, INFN e di Consorzi Interuniversitari
- **1990-1994:** rete **GARR**, prima rete unitaria di Università' e Ricerca
- **1994-1998:** rete **GARR-2**, evoluzione di GARR-1
- **1998-2003:** rete **GARR-B** (Broadband)
- Luglio 2003: il Consortium GARR
- **2003-2008:** rete **GARR-G** (Giganet)

# “il GARR oggi”

---

- Il **Consortium GARR** e' attualmente costituito come associazione di **Fondazione CRUI, CNR, ENEA e INFN** ed e' gestito da un CdA che si avvale di un CTS per richiesta di pareri tecnico-scientifici

# "la Rete GARR"

- GARR e' anche il nome assegnato alla Rete informatica dell' Universita' e della Ricerca Scientifica italiana.
- La Rete GARR interconnette tutte le Universita' (Statali e non) e tutte le sedi degli enti di ricerca scientifica (CNR, ENEA, INFN, ASI, ESA, INAF, INGV, etc.), nonche' Consorzi Interuniversitari, consorzi di ricerca e istituzioni culturali o di ricerca a carattere accademico, scientifico e tecnologico.
- La Rete GARR e' interconnessa (peering) a tutte le Reti della Ricerca mondiali e al Global Internet.

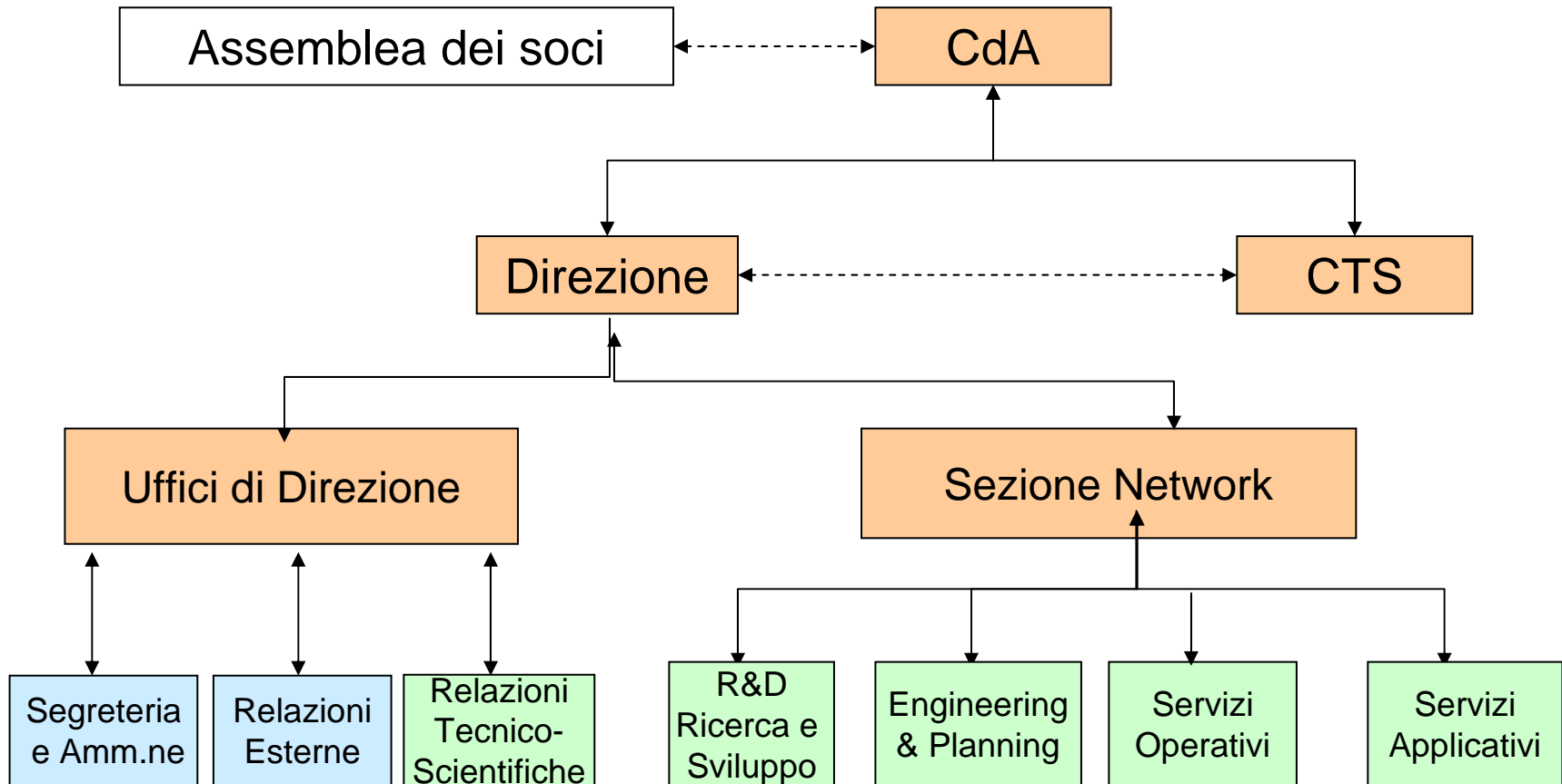
# Enti afferenti alla Rete GARR

---

- Università italiane statali e non statali
- Istituti di Alta Formazione Artistica, Musicale e Coreutica (AFAM)
- Enti nazionali di ricerca CNR, ENEA, INFN, INAF, ASI, INGV, etc.
- Organismi di ricerca vigilati dal MIUR
- Organismi di ricerca vigilati dal Min. Salute (Ospedali e IRCCS)
- Organismi culturali vigilati dal MiBAC (Musei, Biblioteche, Archivi)
- Istituzioni culturali e scientifiche italiane e straniere di rilevante interesse per la comunità scientifica e accademica nazionale.

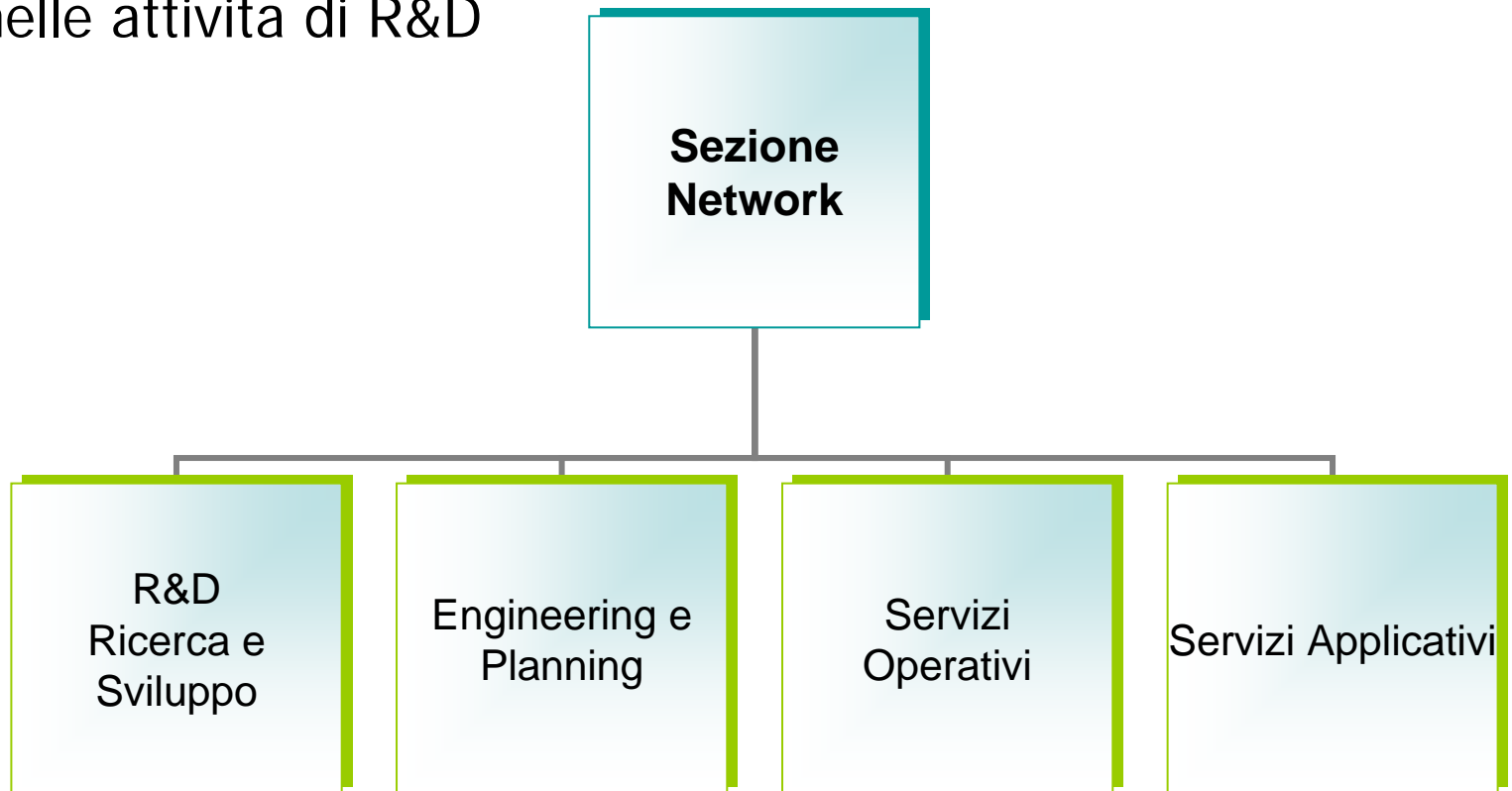


# Organigramma Consortium GARR



# Sezione Network

La Sezione Network cura la progettazione, la gestione operativa e il monitoring della rete GARR, fornisce servizi e supporto agli utilizzatori e alle applicazioni ed è impegnata nelle attività di R&D



# Network (1/4)

---

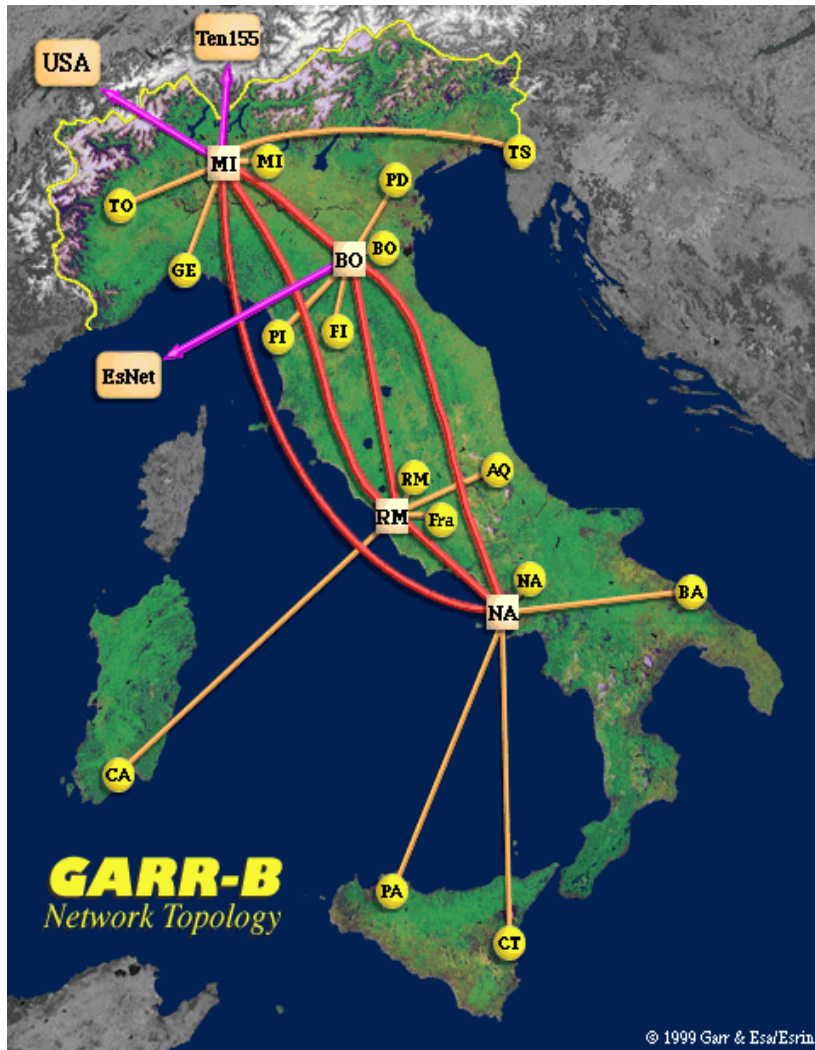
- R&D
  - Attività di sperimentazione e validazione nel campo delle reti ottiche e per l'erogazione di servizi di rete avanzati anche in ambiente multidominio e internazionale
  - GEANT, FEDERICA, EVALSO, ALICE2, EUMEDCONNECT2, EGEE-III ...

- Network Engineering & Planning  
[planning@garr.it](mailto:planning@garr.it)
  - progettazione e engineering di soluzioni tecnologiche finalizzate all'evoluzione della rete
  - supporto agli utilizzatori nella pianificazione di nuovi accessi, servizi e upgrade di banda
  - supporto ai progetti di ricerca con particolari esigenze di connettività
    - LHCOPN, eVLBI, SCOPE, CRESCO, CyberSAR, PI2S2, DEISA, FEDERICA, GEANT, ALICE, EVALSO

- Servizi operativi
  - GARR-NOC [noc@garr.it](mailto:noc@garr.it)
    - interfaccia operativa con gli APM
  - GARR-Operations [operations@garr.it](mailto:operations@garr.it)
    - gestione dei PoP, monitoring, raccolta statistiche, reports
    - sw development
  - GARR-CERT [cert@garr.it](mailto:cert@garr.it)
    - Security, Gestione "incidenti"
  - GARR-LIR [lir@garr.it](mailto:lir@garr.it)
    - allocazione indirizzi IPv4 e IPv6 pubblici, DNS
  - GARR-NIC [nic@garr.it](mailto:nic@garr.it)
    - registrazione di nomi a dominio .it, .eu
  - GARR-AAI, GARR-CA, EduRoam
    - AAI federata, Certification Authority e supporto alla Mobility

- Servizi Applicativi
  - GARR-MIRROR (es. Sourceforge)
  - Usenet News
  - MultiVideo Conferenza
  - GARR-NETCAST: il supporto alla diffusione via Internet degli eventi, anche in alta definizione (DVTS)

# La rete GARR-B (1998-2003)



- Tutte le sedi Universitarie e enti soci collegate
- Architettura di rete magliata solo su 4 POP → 16 POP di concentrazione
- Limitata copertura del territorio nazionale
- Backbone basato su circuiti ATM a 155M e a 34M sulla periferia
- Supporto IPv4
- Collegamento a 155M alla rete TEN-155 → GÉANT
- Modalità di accesso da 2M → 34M (ATM)
- Rete **mono** Operatore (incumbent) con PoP presso centrali Telecom Italia
- Con il Progetto GARR-B inizia lo sviluppo delle reti Metropolitane (**MAN**)

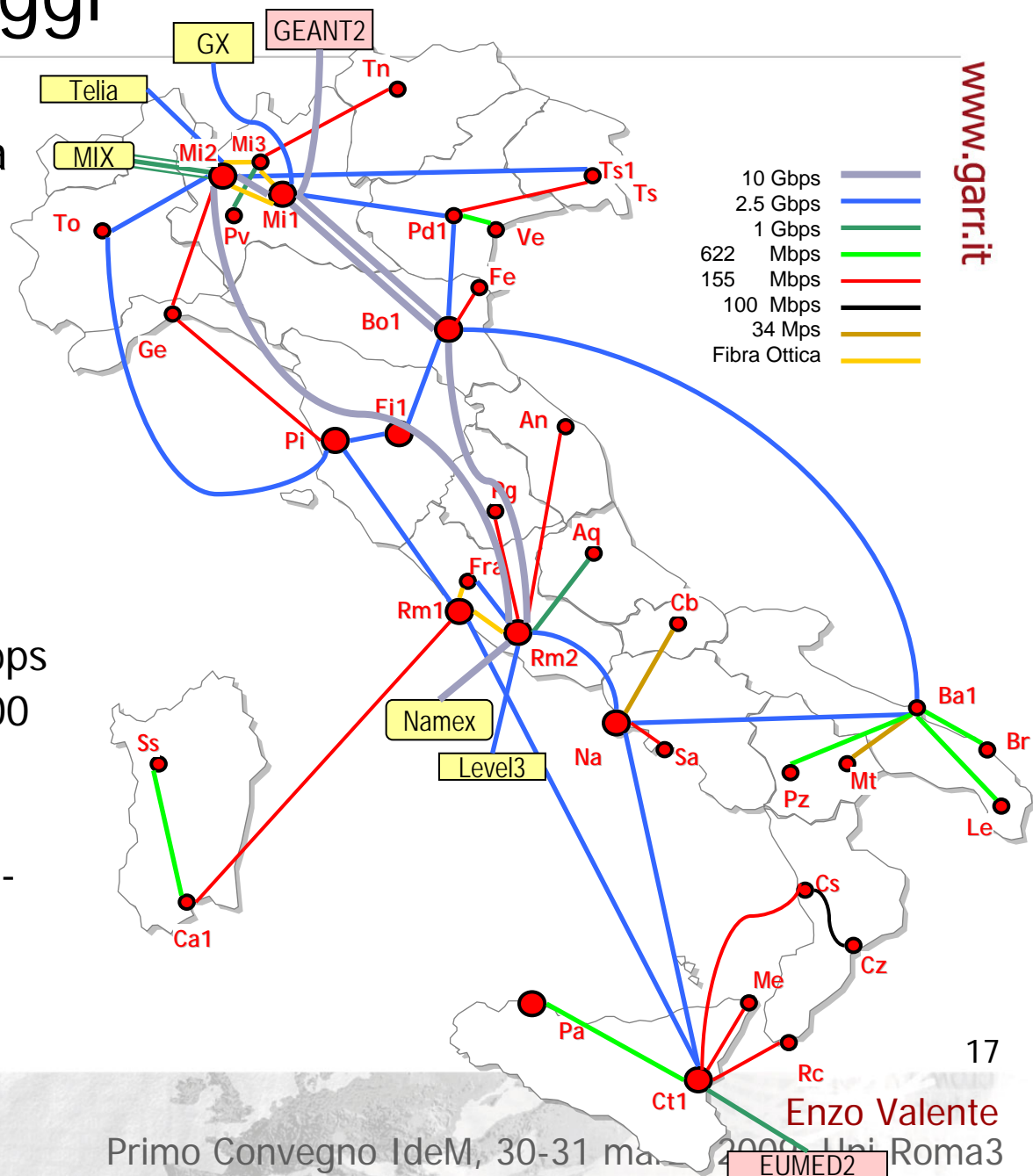
# GARR-G: criteri di progettazione

- Modellata sulle esigenze degli utenti
- Portare i PoP nei **baricentri** di traffico, distribuiti sul territorio e in **casa degli utenti** (Laboratori e Università) per garantire la **neutralità** agli operatori emergenti
  - Riduzione dei costi dei circuiti di accesso
- il PoP di **GEANT** collocato con il Giga-PoP GARR a Milano
  - per raggiungere in fibra le altre NREN in Europa e nel mondo
- un backbone **overprovisioned** rispetto all'accesso e consentire un'evoluzione da **2.5Gbps** iniziali a **10Gbps** (router adeguati)
- Spesa costante a fronte di un incremento di capacità e ottimizzazione dei costi



# La rete GARR-G oggi

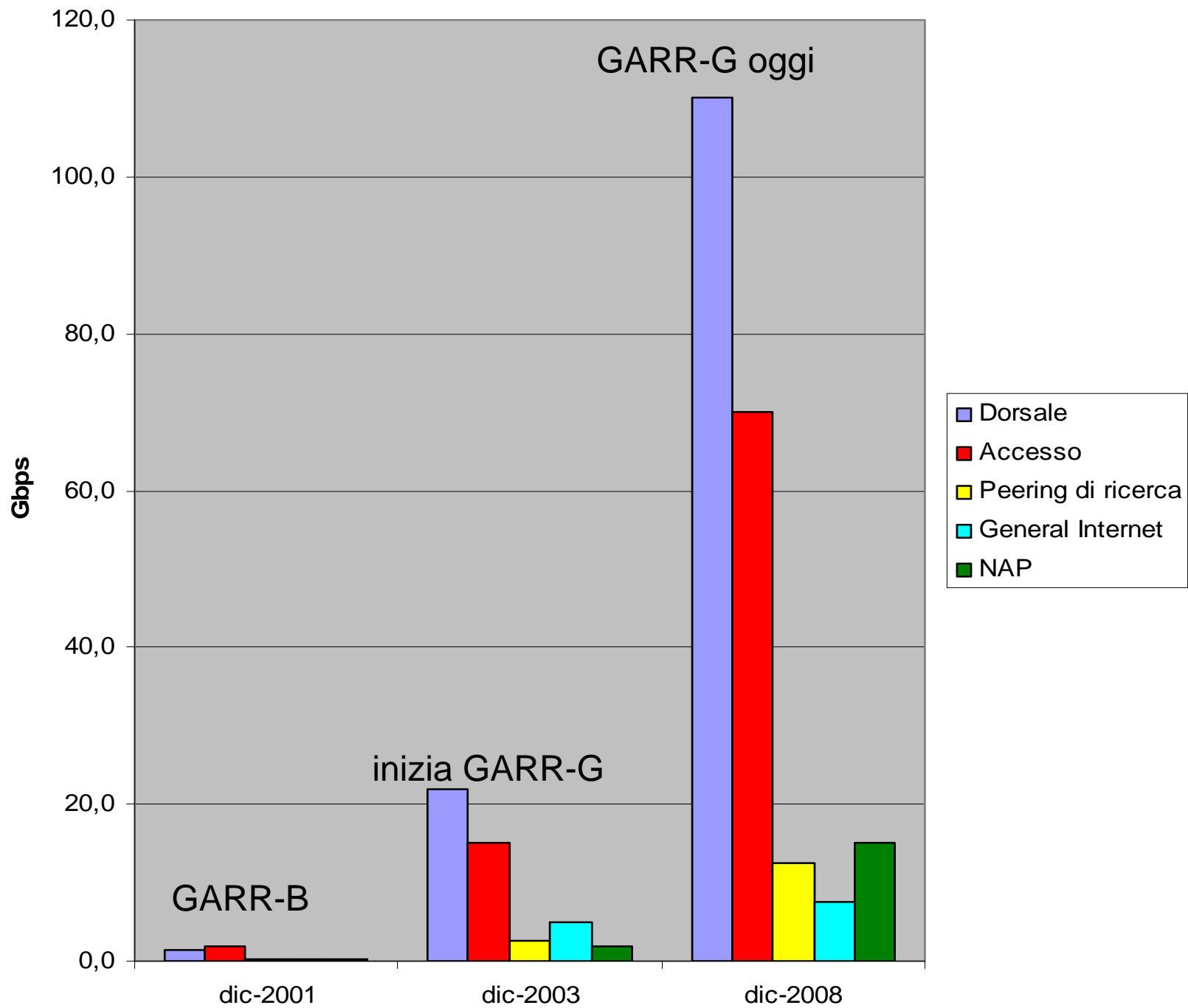
- 43 PoP (oltre 90% ospitati da Università e enti di ricerca)
- Capacità aggregata IP del backbone
  - ~ 110Gbps
  - N. link di backbone: 62
- Capacità aggregata IP link di accesso
  - ~ 70Gbps
  - Accessi da 2Mbps → 10Gbps
  - N. link di accesso: oltre 400
- 8 operatori TLC nazionali
  - TI, Infracom, Fastweb, Atlanet Interoute, Wind, BT-Italia, COLT
- Diversi operatori TLC locali
  - Municipalizzate, ecc



# I collegamenti di Peering

- Peering IP con le reti di Ricerca internaz.  
circa 12.5Gbps via GEANT
- Peering IP di commodity:
  - International Internet via GX,Telia,Level3  
circa 7.5Gbps
  - National Internet via MIX, NAMEX, TIX, Top-ix...  
circa 20Gbps
- Circuiti dedicati end-to-end a livello internazionale per progetti di Ricerca (LHCOPN, eVLBI, DEISA, FEDERICA,...)  
circa 35Gbps complessivi

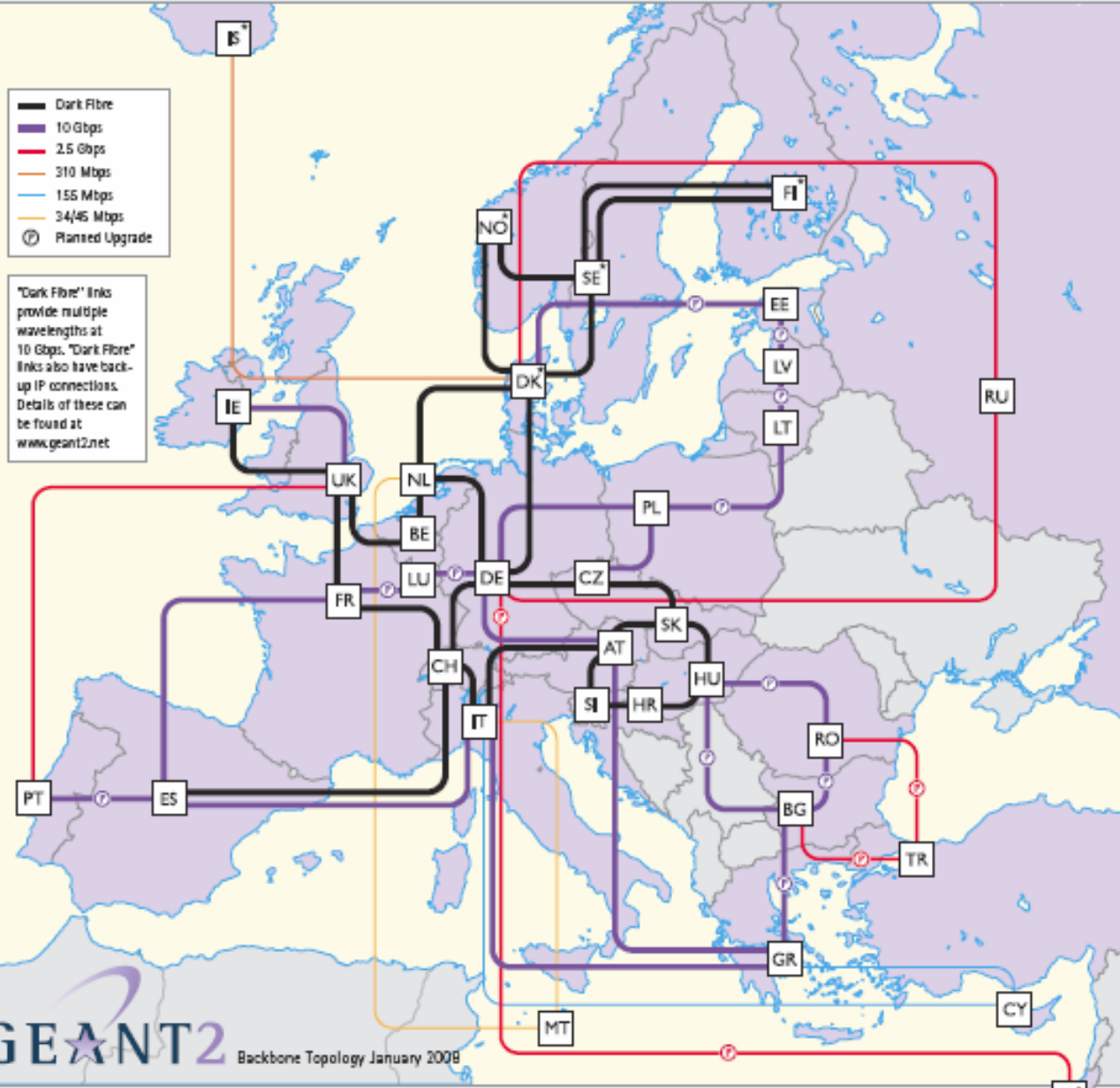
# La capacità della rete da GARR-B a oggi



# La rete pan-europea delle Università e della Ricerca: GEANT2

[ottimizzazione dei servizi e dei costi per l'interconnessione a livello Europeo]

www.garr.it



- Progetto GN2 cofinanziato al 50% dalla CE
- buona parte della rete GEANT2 è basata su fibra ottica ad uso esclusivo a lungo termine (linee nere)
- 20 NREN connesse in fibra ottica tra cui la rete GARR
- 15 NREN connesse via circuiti su "lambda" o SDH forniti da operatori TLC
- GARR è partner del progetto GN2
- GARR è socio di DANTE, l'org. che gestisce la rete GEANT

# The NREN Policy Committee

1. **ACOnet** (Austria)
2. **ARNES** (Slovenia)
3. **BELNET** (Belgium)
4. **BREN** (Bulgaria)
5. **CARNet** (Croatia)
6. **CESNET** (Czech Republic)
7. **CYNET** (Cyprus)
8. **DFN** (Germany)
9. **EENet** (Estonia)
10. **FCCN** (Portugal)
11. **GARR** (Italy)
12. **GRNET** (Greece)
13. **HEANet** (Ireland)
14. **HUNGARNET** (Hungary)
15. **IUCC** (Israel)
16. **JANET** (United Kingdom)
17. **JSCC** (Russia)
18. **LITNET** (Lithuania)
19. **NORDUnet** (Nordic Countries -  
Denmark, Finland, Iceland, Norway,  
Sweden)

20. **PSNC** (Poland)
21. **RedIRIS** (Spain)
22. **RENATER** (France)
23. **RESTENA** (Luxembourg)
24. **RoEduNet** (Romania)
25. **SANET** (Slovakia)
26. **SigmaNet** (Latvia)
27. **SURFNET** (Netherlands)
28. **SWITCH** (Switzerland)
29. **ULAKBIM** (Turkey)
30. **UoM** (Malta)

#### PLUS NON-VOTING MEMBERS:

31. **DANTE** (Delivery of Advanced Network Technologies to Europe Ltd.)
32. **TERENA** (Trans-European Research & Education Networking Association)

#### PERMANENT OBSERVERS:

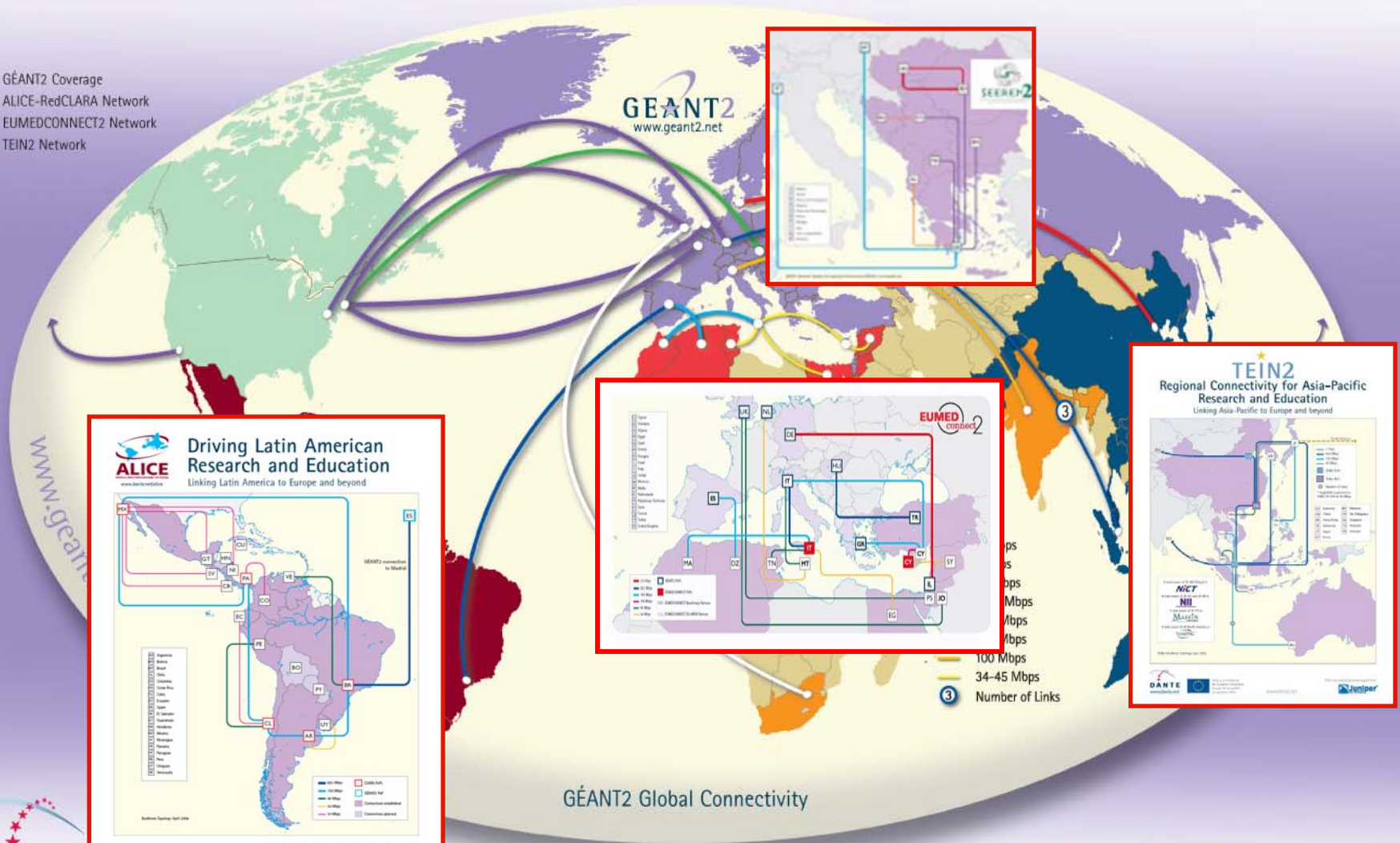
33. **AMRES** (Serbia)
34. **MARNET** (FYR of Macedonia)
35. **CERN** (European Organization for Nuclear Research)



# GEANT2: La rete pan-europea al centro del sistema mondiale delle reti della Ricerca



- GEANT2 Coverage
- ALICE-RedCLARA Network
- EUMEDCONNECT2 Network
- TEIN2 Network



**Driving Latin American Research and Education**  
 Linking Latin America to Europe and beyond

**ALICE**  
[www.alice.net](http://www.alice.net)

Map showing connections between Latin American countries (e.g., BR, CL, CO, CR, CU, EC, GT, HA, HN, MX, NI, PA, PE, PR, PY, SV, TN, VE) and Europe. Includes a legend for link types and speeds.

**EUMEDconnect2**

Map showing connections across Europe and the Mediterranean region. Includes a legend for link types and speeds.

**TEIN2**  
 Regional Connectivity for Asia-Pacific Research and Education  
 Linking Asia-Pacific to Europe and beyond

Map showing connections between Asia-Pacific countries (e.g., AU, CN, HK, IN, JP, KR, MY, NZ, SG, TH, TW, VN) and Europe. Includes a legend for link types and speeds.

# Le attività di R&D del GARR

Le attività sono svolte soprattutto in ambito internazionale attraverso [progetti europei co-finanziati](#), con lo scopo di

- [Sviluppare](#) per un utilizzo immediato le [tecnologie ed i servizi](#) per le reti della ricerca (per esempio il progetto GN2 per la rete GEANT)
- Fornire [supporto avanzato](#) ai ricercatori nel campo delle reti e dei servizi e studiare modelli di [evoluzione](#) della rete (progetto FEDERICA)
- Fornire [supporto](#) allo sviluppo dei [sistemi di griglia](#) (progetto EGEE-3)

# Le attività di R&D - Progetto GN2-GÉANT2

[Progettazione e Realizzazione della rete della ricerca pan-europea GEANT2]

Progetto quinquennale (I3) del 6<sup>o</sup> Programma Quadro (termine nel 2009) a cui partecipano tutte le NREN Europee. Le attività di ricerca e sviluppo più significative sono tutte in ambiente **multidominio** (di competenza e gestione di rete) e sono:

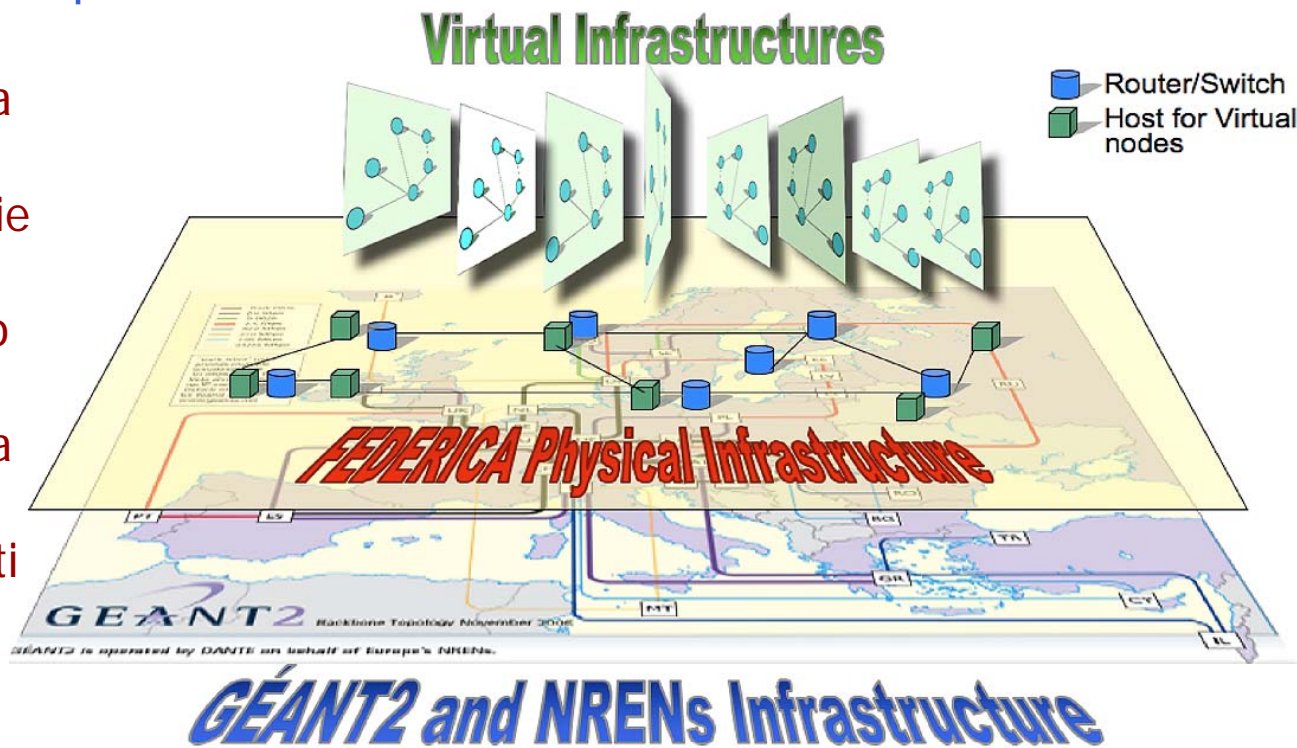
- Sistema di **Monitoring** (PerfSONAR) per il controllo dei circuiti **end-to-end** (da quelli fisici "lightpath" a quelli logici basati su MPLS e IP)
- Procedure di gestione degli incidenti di **Sicurezza** tra le diverse NREN, con sviluppo di strumenti di monitoring "attivo" per identificare minacce di sicurezza in tempi brevi (es. DDoS)
- Servizio di **Bandwidth on demand**, (AutoBAHN) per l'erogazione (semi)-automatica di circuiti (1 e 10Gbps) end to end
- Sviluppo delle **fibres transfrontaliere** (Cross Border Fiber) a complemento della infrastruttura GEANT2
- **cNIS**: database topologico multidominio per l'erogazione dei servizi end-to-end
- **I-Share**: procedure operative per il set up, il rilascio e la gestione dei circuiti end-to-end (GARR è leader dell'attività)
- Performance Enhancement Response Team (**PERT**), un NOC federato a livello europeo (NREN), per l'assistenza agli utenti su problemi di prestazioni delle applicazioni



# Le attività di R&D - Progetto FEDERICA

- Progetto del 7<sup>^</sup> Programma Quadro di 30 mesi con inizio gennaio 2008 con 20 partner. GARR è il **coordinatore** del progetto
- Il progetto ha lo scopo di creare **un'infrastruttura** composta da apparecchiature di rete, circuiti e nodi di calcolo capaci di virtualizzazione, per accogliere attività sperimentali su **architetture e nuovi protocolli per l'Internet del futuro**

- L'infrastruttura è **agnostica** nelle tecnologie utilizzate, ed estesa a livello europeo.
- È composta da circuiti Gigabit Ethernet forniti da GÉANT



# Le attività di R&D - Progetto EGEE-3

- EGEE-III è un progetto biennale del 7<sup>o</sup> Programma Quadro, iniziato a luglio 2008, che ha lo scopo di estendere ed ottimizzare l'infrastruttura di griglia a livello europeo.
- GARR è coinvolto nelle joint research activity e service activity che si occupano di aspetti legati
  - alla interconnessione attraverso la rete dei siti di griglia
  - al monitoring end to end del traffico
  - agli aspetti di compatibilità con il protocollo IPv6 dei codici di gestione del sistema di griglia



# Da GARR-G a GARR-X

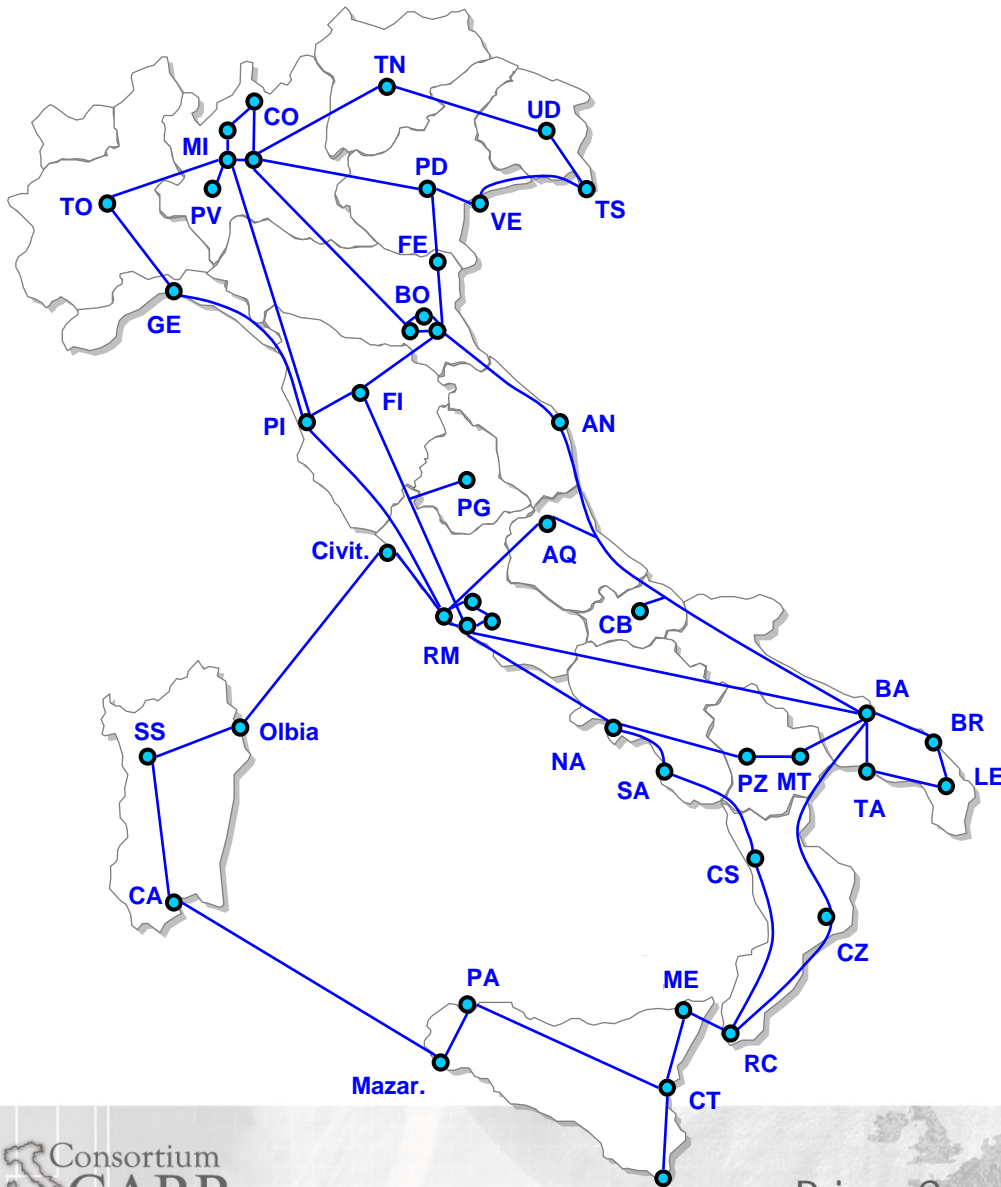
---

- GARR-X è il progetto che guiderà l'evoluzione della rete dell'università e della ricerca italiana per i prossimi (almeno) 6 anni
- La rete GARR-X sarà operativa a partire da metà 2009 (GARR-X Fase0)
- Migrazione in continuità di servizio con l'attuale rete GARR-G

# Caratteristiche della rete GARR-X

- Evoluzione dell'infrastruttura a costi incrementali ridotti
- Flessibilità nella risposta alle richieste (attuali e future) degli utilizzatori
  - Possibilità di ritagliare su GARR-X reti dedicate a sedi o gruppi di utilizzatori remoti per il supporto di servizi/applicazioni specifiche
- Integrazione con reti di Campus, reti Metropolitane e reti Regionali
- Accesso a basso costo e banda garantita
  - FastEthernet, 1Gigabit e 10Gigabit Ethernet in
    - fibra (soluzione preferita  $\geq 1\text{Gbit/s}$ )
    - circuito diretto ( $<1\text{Gbit/s}$ )
    - aggregazione di circuiti tramite reti di operatori ( $<100\text{Mbit/s}$ )

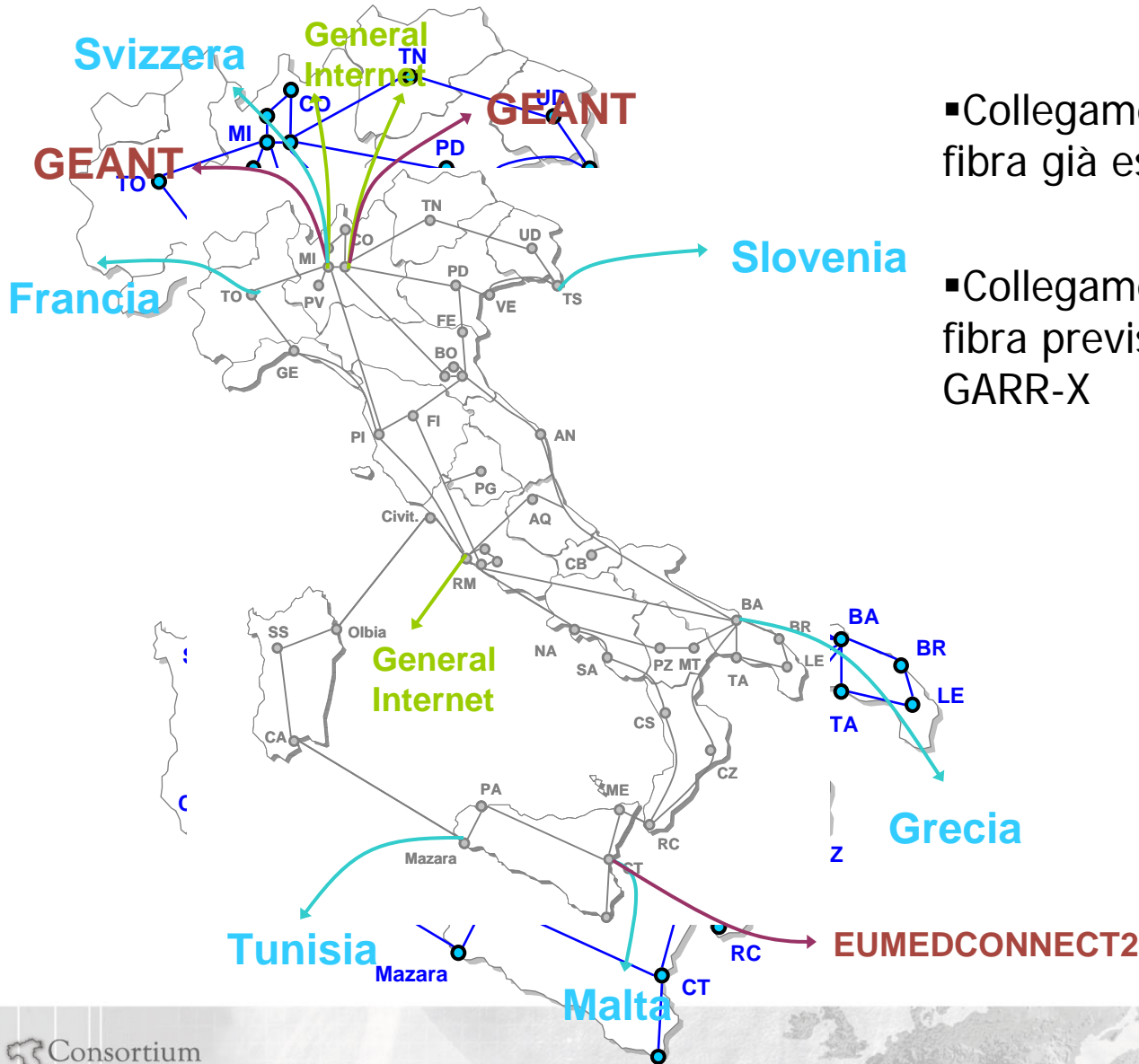
# Infrastruttura di fibra di dorsale di GARR-X



Alcune cifre di sintesi

- 45 PoP GARR principali
  - 99% co-locati con sedi utente
- 60 apparati trasmissivi
  - 150 nodi di amplificazione (uno ogni 70 km di fibra)
- 10.500 km fibre di dorsale
- 1.500 km fibre di accesso (non presenti in figura)

# Collegamenti in fibra con le altre reti della ricerca



- Collegamenti internazionali in fibra già esistenti
- Collegamenti internazionali in fibra previsti nel corso di GARR-X





**GARR**

The Italian Academic & Research Network

www.garr.it

**GARR CA**

**Certification Authority GARR**

<http://ca.garr.it>



# GARR Certification Authority (CA)

- **Rilascia certificati X.509**
  - per persone fisiche (certificati personali)
  - per macchine server o servizi (certificati server)
- **I certificati sono la “firma digitale” per**
  - firmare, cifrare, verificare l’integrità,...
  - “garantiscono” l’identità di utenti e servizi



# GARR Certification Authority (CA)

- **i certificati personali**
  - già più di uno “personale” in tasca (CI elettronica, CF, Tessera Sanitaria...)
  - abbiamo più di una “credenziale” di accesso a servizi sul nostro PC, anche in formato “certificato”.
  - i ruoli dell’intestatario sono diversi:
    - **Cittadino, contribuente, assistito, ...**
    - **utente di una biblioteca, ricercatore del progetto, ...**
  - GARR CA emette **gratuitamente** certificati personali per gli utenti GARR **usabili per i propri ruoli nella comunità accademica e della ricerca**

# GARR Certification Authority (CA)

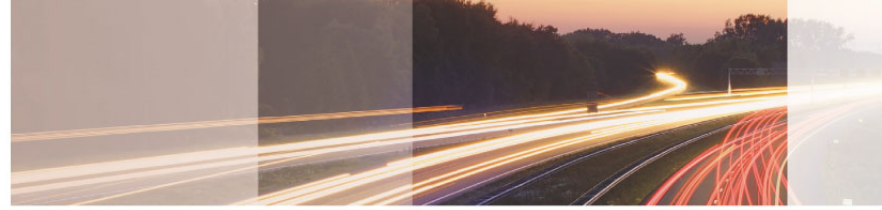
- i certificati server
  - Per le macchine, la GARR CA rilascia gratuitamente:
    - Certificati server firmati solo da GARR CA
    - Certificati server firmati da Globalsign (servizio Scientific Certificate Service, TERENA, GARR ed altre reti della ricerca)
      - automaticamente riconosciuti da tutti i browser
      - eliminano il problema del popup (molto serio nei nuovi browser)
      - Un singolo certificato Globalsign / Verisign richiesto autonomamente da voi vi costerebbe > 100\$/anno

# GARR Certification Authority (CA)

- i certificati emessi da GARR CA NON hanno validità legale (sono una “firma digitale debole”)
  - scelta deliberata dopo attenta valutazione pro/contro
  - di CA per firma digitale forte (legale) ce ne sono molte, ma:
    - i certificati “a valore legale” in Italia NON hanno validità all’interno della comunità accademica e della ricerca internazionali
    - non possono essere usati per definire i “ruoli” accademici
- GARR CA segue gli (elevati) standard IGTF per le CA abilitate a rilasciare certificati riconosciuti dai progetti grid
- GARR CA è la sola che permette di estendere la “catena di fiducia” (trust) a livello internazionale (“confederazioni” accademiche e della ricerca internazionali)

# GARR Certification Authority (CA)

- Per usare GARR CA
  - istituire una "Registration Authority" presso la propria istituzione
    - Un paio di persone che, tra le altre attività, abilitate a gestire le richieste dei certificati a nome dei vostri utenti
  - circa 70 Registration Authority: già presente in quasi tutte le principali Università ed Enti di Ricerca
  - corsi di istruzione per utenti e RA
    - Dal vivo, Documentazione, tutorial, video...



**GARR**

The Italian Academic & Research Network

www.garr.it

# GARR IDEM

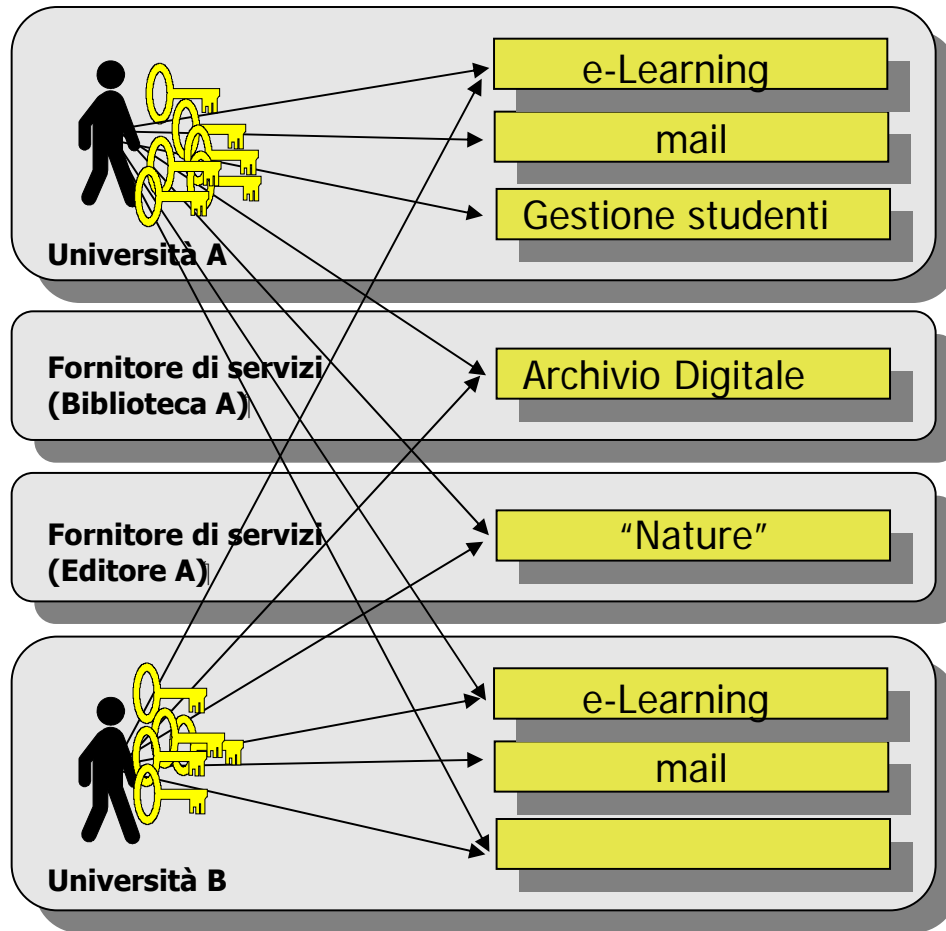
Servizio Federato di Autenticazione e  
Autorizzazione (AAI) GARR

<http://idem.garr.it>



# Struttura Autorizzazione Autenticazione (AAI)

## Metodo "tradizionale"

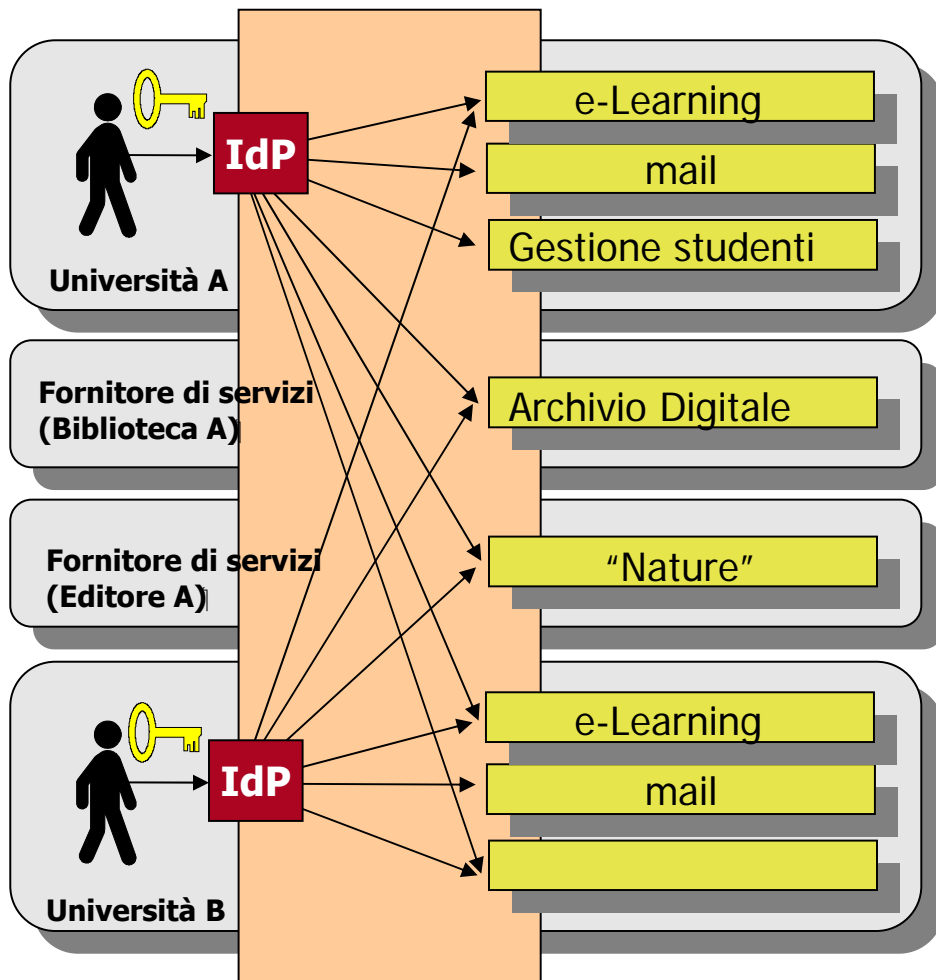


- L'identità e i dati personali degli utenti sono noti al di fuori della propria organizzazione
- I fornitori di servizi devono mantenere un db utenti
  - privacy
- Gli utenti devono gestire molti account
  - dati inconsistenti
- Debolezza credenziali di accesso

**Gestione complessa ed insicura!**

# Struttura Autorizzazione Autenticazione (AAI)

## Metodo "federato"



- L'identità e i dati personali dell'utente sono conservati solo dalla propria organizzazione
- il Fornitore di Credenziali (Identity Provider - IdP) è locale
- I fornitori di servizi non devono avere un db di tutti gli utenti
- Un solo login
- Autorizzazione basata su attributi / ruoli

**RISOLVE!**

# Vantaggi per tutti del modello "federato"

## **Organizzazioni:**

Maggiore controllo sul processo di autenticazione e autorizzazione  
Può essere usata anche per proteggere le risorse interne  
Investimento iniziale, ma a regime produce risparmi.

## **Fornitori di servizi:**

Non devono gestire db utenti  
Maggiore flessibilità di autorizzazione: istituzione, ruolo, ecc. ecc.  
Dati utente sempre aggiornati  
Minori problemi di gestione dati personali

## **Utenti:**

Maggiore privacy: dati personali rilasciati solo se necessario  
Utilizzo di credenziali uniche  
Accesso alle risorse online da (quasi) ovunque  
Meno password da ricordare!





Shibboleth

- Nata a Gennaio 2008
- dal 1/1/09 "servizio IDEM"
- Basata su standard (Shibboleth)
- Già 15 fornitori di credenziali (IdP) (oltre 2 milioni di utenti)
- 9 fornitori di servizi e contenuti (SP)

# Ruolo e Supporto del GARR in IDEM

- **GARR gestisce la federazione**
  - ruolo di notaio
  - accordi bilaterali con i membri della federazione
- **Supporto Tecnico**
  - WAYF (where are you from) server
  - Metadati della federazione
  - Server WEB della federazione
  - Certification Authority
- **Rapporti Internazionali**
  - Gestione della catena di fiducia (trust) internazionale
  - Confederazioni internazionali nella comunità accademica e della ricerca

- Sono le università in toto che debbono federarsi, e NON i singoli dipartimenti
- Per usare la federazione:
  - Istituire il proprio IdP
    - Spesso basta aggiungere un modulo ai sistemi esistenti e funzionanti!
  - Dotare di interfaccia di “fornitore di servizio” i servizi che si desiderano offrire
    - anche nessuno!
  - Aderire formalmente alla federazione stessa
- IdP ospitato e per i “senzatetto”

Tanti ringraziamenti a tutti coloro  
che hanno reso possibile la realizzazione del  
progetto IdeM

Fondamentale, per il successo dell'iniziativa,  
il ruolo  
della "assemblea dei soci delle Federazione"  
e del "comitato di indirizzo" (advisory  
committee)

Tanti auguri al  
“GARR Operation Committee”  
coordinato da Lalla Mantovani  
con cui collaborano  
Barbara Monticini, Simona Venuti,  
Maria Sole Scollo e Andrea Pinzani  
(GARR-CERT e GARR-CA in Firenze);  
e il team di supporto GARR in Roma.

grazie per l'attenzione  
(ma non dimenticate di  
riempire il questionario!)  
e buon lavoro